Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

GICAN

Ce numéro vous est offert par le Groupement des Industries de Construction et Activités Navales

Red Team
INTRUSION COMMANDITÉE

POLITIQUE NATIONALE
Jérôme Notin, Directeur général du dispositif national d'assistance Cybermalveillance.gouv.fr

N°43 - Prix : 24 € TTC - Trimestriel : avril, mai, juin 2018

HS2
Hervé Schauer Sécurité

Formation Vie privée, Droit de la cybersécurité et Continuité d'activité

PROGRAMME

Vie privée et droit de la cybersécurité

RGPD :
RGPD/GDPR / Réglement Européen sur la Protection des Données personelles
DPO :
Formation DPO / Privacy Implementer
PIA :
PIA / ISO29134 / Appréciation des impacts sur la vie privée
SECUSANTE :
Protection des données de santé et vie privée
SECUDROIT :
Droit de la cybersécurité
SECUCLOUD :
Sécurité du cloud

Continuité d'activité

RPCA :
Formation RPCA
ISO22LA :
ISO22301 Lead Auditor
ISO22LI :
ISO22301 Lead Implementer

idcomm.fr

+33 644 014 072

www.hs2.fr

formations@hs2.fr

RED TEAM : LES ÉQUIPES SÉCURITÉ À L'ÉPREUVE DU FEU

Les jeux de guerre ont toujours excité les Hommes, petits ou grands, en particulier les garçons. D'ailleurs, pour ceux qui ont fait l'armée, tous se rappellent des manœuvres durant lesquelles les Rouges, souvent les « méchants », allusion non dissimulée aux « Communistes », soviétiques, chinois… se battaient contre les Bleus, généralement les « gentils », bien sûr les occidentaux ! C'est ainsi sans doute qu'a germé, au fil du temps, dans l'esprit des militaires américains l'idée d'appliquer ces simulations à la cybersécurité. Des équipes Red Team ont donc progressivement été mises sur pied, avec comme objectif d'infiltrer les équipes bleues, alias les Blue Team, bien sûr en prévenant le minimum de personnes afin d'éviter les fuites… Effectivement, quel meilleur entraînement que l'attaque par surprise pour vérifier l'aptitude des équipes à répondre à une « invasion » ?

Plusieurs années après la naissance de cette méthode, nos experts constatent que le niveau de sécurité des entreprises s'est quelque peu renforcé. Toutefois, les Blue Team sont aujourd'hui encore trop perméables et se font percer trop facilement, surtout face à des menaces protéiformes et des attaquants qui ne cessent de perfectionner leurs techniques. De leur côté, les vulnérabilités logiques sont multiples et ne cessent de gagner en sophistication. Mais plus grave encore : la sécurité physique, bien qu'adressée depuis plus longtemps en entreprise, laisse toujours à désirer dans bon nombre de structures. D'ailleurs, les portes de sécurité, quand il y en a, sont souvent laissées entrouvertes pour simplifier, entre autres, les allées et venues des fumeurs dans l'entreprise… Sans compter les autres incontournables vecteurs d'infection, comme la fameuse clé USB ramassée par terre ! Un dénominateur commun à tout cela : l'humain, qui ne va pas pouvoir s'empêcher de contourner un système de sécurité pour se simplifier la vie, ou de récupérer une « merveilleuse » trouvaille qui lui tend les bras… Ainsi, les Red Team parviennent quasiment toujours à gagner à la fin, au grand dam des RSSI et DSI qui voient au fil des tests s'éloigner leur recherche de sécurité absolue, à l'instar de la quête du Graal.

LISTE DES ANNONCEURS

6cure	31
Bachmann	51
Club Décision DSI	2
Conscio	15
Cyberwatch	35
Deloitte	30, 34, 38
Forum Sécurité@Cloud	24
France Cybersecurity	14
GS Days	8
GS Mag Data Center	48
Hacking Lab	9
HS2 (Hervé Schauer Sécurité)	20, 2ème et 3ème de couverture
I-Tracing	17
ITrust	11
Kaspersky	4ème de couverture
Les Assises de la Sécurité	42
Mobility For Business	6
Oveliane	39
The GreenBox	22
Usercube	4
WattDesign	49

Toute reproduction intégrale ou partielle, faite sans le consentement de l'auteur ou des ayants droit ou ayant cause est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque. (article L122-4 du code de la propriété intellectuelle).
Cette publication peut être exploitée dans le cadre de la formation permanente. Toute utilisation à des fins commerciales du contenu éditorial fera l'objet d'une demande préalable auprès du Directeur de la publication.

REVUE TRIMESTRIELLE
N°43 – avril, mai, juin 2018
www.globalsecuritymag.fr et
www.globalsecuritymag.com
ISSN : 1959 - 7061
Dépôt légal : à parution
Editée par SIMP
RCS Nanterre 339 849 648
17, avenue Marcelin Berthelot
92320 Châtillon
Tél. : +33 1 40 92 05 55
e-mail : marc.jacob@globalsecuritymag.com

REDACTION
Directeur de la Publication :
Marc Brami
Rédacteur en chef :
Marc Jacob
Rédactrice :
Emmanuelle Lamandé
Mise en page :
S.I.M. Publicité
Ont collaboré à ce numéro :
Olivier Iteanu, Jérôme Notin, Virgile Jarry, Quentin Heyler, Anthony Coquer, Arnaud Soullié et Charles Ibrahim
Traduction : Ian Nathan
Assistante : Sylvie Levy
Responsable technique :
Raquel Ouakil
Photos :
Norbert Martiano, Marc Jacob
Comité scientifique :
Pierre Bagot, Francis Bruckmann Eric Doyen, Catherine Gabay, François Guillot, Olivier Iteanu, Dominique Jouniot, Patrick Langrand, Yves Maquet, Thierry Ramard, Hervé Schauer, Michel Van Den Berghe, Bruno Kerouanton, Loïc Guézo et Valentin Jangwa
In Memoriam, notre regretté Zbigniew Kostur

PUBLICITE
SIM Publicité
Tél. : +33 1 40 92 05 55
e-mail : ipsimp@free.fr
Images de couverture :
©adike

IMPRESSION
Imprimerie Moutot
33-37, rue Hyppolyte Mulin
92120 Montrouge
Tél. 01 46 57 79 79
Contact : Sébastien Bellut
e-mail : sebastien@imprimeriemoutot.fr
Imprimé avec des encres végétales sur papier éco-responsable certifié PEFC par un imprimeur adhérent à Imprim'vert selon le procédé CTP sans chimie.

ABONNEMENT
Prix au numéro :
24 € TTC (TVA 20%)
Abonnement annuel :
60 € TTC (TVA 20%)

CLUB DECISION DSI

1er Club Français de décideurs informatiques & télécoms
1250 MEMBRES

Véronique Daval
Présidente

Un réseau indépendant et privé au sein duquel siègent 12 DSI ambassadeurs de leur secteur d'activité

Julien Daval
Vice-Président

LES MEMBRES DU BUREAU ET AMBASSADEURS DU CLUB

Armand ASSOULINE
CIO
MSC FRANCE

Christian DOGUET
DSI
CHAINE THERMALE DU SOLEIL

Trieu HUYNH-THIEN
DSI ADJOINT
CENTRE GEORGES POMPIDOU

Lionel ROBIN
DSI
GROUPE LA RESERVE

Gilles BERTHELOT
RSSI
GROUPE SNCF

Damien GRIESSINGER
CTO
EPPO

Bertrand LENAIN
DSI
CCI DE SEINE ET MARNE

Dominique TROUVE
DSI
HÔPITAUX AVICENNE

Christophe BOUTONNET
SOUS-DIRECTEUR SCHÉMA DIRECTEUR ET POLITIQUE SI

Christophe GUILLARME
DSI
GROUPE AB TÉLÉVISION

Stéphane MALGRAND
DSI
Laboratoire national de Métrologie et Essais

Claude YAMEOGO
ARCHITECT SI
ALSTOM

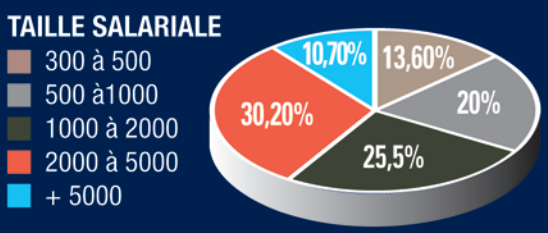
Le Club accompagne les DSI à faire les bons choix technologiques et aligner l'informatique sur la stratégie de l'entreprise

EVOLUTION DU CLUB DECISION DSI

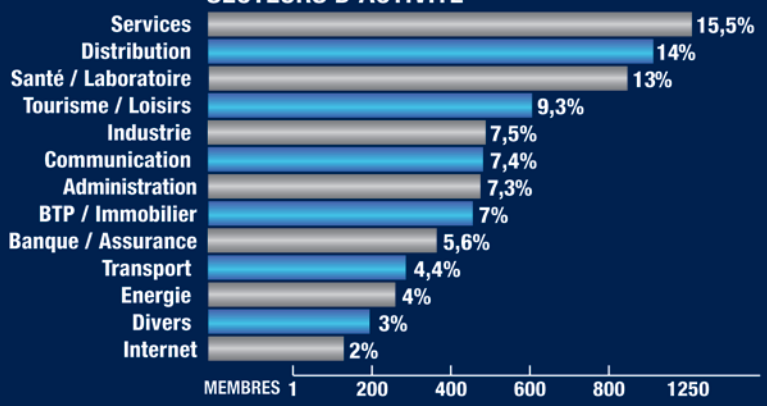
LES MEMBRES DU CLUB

1200 CIO, DOSI, DSI, DI Membres du Club, sociétés de + 300 salariés PARIS/IDF

TAILLE SALARIALE



SECTEURS D'ACTIVITÉ



CLUB DECISION DSI • 33, Rue Galilée 75116 Paris • Tél +33 1 53 45 28 65
www.clubdecisiondsi.fr
Contact : Véronique DAVAL - Présidente
veronique.daval@decisiondsi.com

@clubdecisiondsi

www.imstudio.fr

EDITORIAL

BY MARC JACOB

RED TEAMS: SECURITY TEAMS FACING A TRIAL BY FIRE

War games have always fascinated people, young and old, mostly boys of course. All those who did their military service, will remember the manoeuvres during which the Reds, often the "bad guys", undisguised allusion to the Soviet, Chinese ... "Communists", would fight against the Blues, the Westerners, naturally the "good guys"! Unsurprisingly over time there grew up, in the minds of the American military, the idea of applying these simulations to cybersecurity. Increasingly Red Teams were set up, with the goal of infiltrating Blue Teams, informing as few as possible to avoid leaks ... Surely, what better training than a surprise attack to test the ability of teams to respond to an "invasion"?

Several years after the emergence of this strategy, our experts observe that the level of enterprise security has improved to a certain extent. However the Blue Teams are still too penetrable today and are breached too easily, especially in the face of protean threats and attackers who constantly improve their techniques. Logical vulnerabilities, on the one hand, are diverse and are increasingly sophisticated. But even more serious is physical security, an enterprise issue which, despite having been tackled for much longer, remains insufficient in many organisations. For example enterprise security doors, when there are any in place, are often left unlatched to simplify, among other things, the comings and goings of staff smokers ... Not to mention other notorious vectors of infection, such as the egregious USB stick found on the ground! The common denominator underlying all this: people. It makes life so much easier if you can just bypass a security system, and it is so tempting to pick up that little "treat" that you happen to stumble upon. It follows that as the tests march on the Red Teams almost always win at the end, much to the chagrin of the CISOs and CIOs whose quest for the Holy Grail of total security slowly slips away over time.

USERCUBE

GOUVERNANCE et ADMINISTRATION des IDENTITÉS

SOLUTION DE NOUVELLE GÉNÉRATION

ON PREMISE & AZURE

- Cycle de vie des Identités
- Gestion des règles et des rôles
- Role Modeling / Role Mining
- Workflow d'administration (demande et validation)
- Recertification des accès
- Contrôles de sécurité automatisés
- Audit, traçabilité et reporting
- Provisioning automatique et ouverture de tickets
- Self-service de mot de passe

www.usercube.com | contact@usercube.com | 09 72 31 03 15

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

THÉMA

18

RED TEAM

SOMMAIRE

01 **Édito :** Red Team : les équipes sécurité à l'épreuve du Feu
03 **Editorial :** Red Teams: security teams facing a trial by fire
09 **Agenda**

10 **POLITIQUE NATIONALE**
- **Cybermalveillance.gouv.fr lance le premier volet de son kit de sensibilisation**
Par Jérôme Notin, Directeur général du dispositif national d'assistance Cybermalveillance.gouv.fr

12 **RGPD**
- **Notifier une violation de données personnelles : quand, où, quoi, comment ?**
Interview de Matthieu Grall, Chef du service de l'expertise technologique, CNIL
Par Marc Jacob et Emmanuelle Lamandé

16 **CHRONIQUE JURIDIQUE**
- **Red Team, une prestation bien de notre époque**
Par Olivier Iteanu, Avocat, Chargé d'enseignement à l'Université de Paris I Sorbonne

18 **THÉMA - RED TEAM**
- **Red Team : pensez comme un attaquant !**
Par Marc Jacob et Emmanuelle Lamandé
- **Red Team & ingénierie sociale : à tous les coups l'on gagne !**
Par Marc Jacob et Emmanuelle Lamandé
- **Red Team : retour sur quelques anecdotes croustillantes !**
Par Marc Jacob et Emmanuelle Lamandé
- **Have I Been Pwned ? – Yes you have !**
Par Virgile Jarry, auditeur en cybersécurité chez ACCEIS

40 **CHRONIQUE TECHNIQUE**
- **Sécurisation de l'IoT industriel déployé à grande échelle**
Par Quentin Heyler, expert en sécurité opérationnelle pour le cabinet ERIUM

44 **SENSIBILISATION**
- **Le GRAND QUIZZ de sensibilisation - Eté 2018**
Par Arnaud Soullié, Manager, et Charles Ibrahim, Consultant - Wavestone

46 **DATA CENTER**
- **Certification HDS : la pilule risque d'être difficile à avaler pour certains opérateurs**
Par Marc Jacob et Emmanuelle Lamandé
- **L'hébergement neutre en colocation et la responsabilité relative à la protection des données**
Par Anthony Coquer, Département Sécurité & Organisation, Lexing Alain Bensoussan Avocats

10 POLITIQUE NATIONALE

12 RGPD

16 CHRONIQUE JURIDIQUE

18 THÉMA

40 CHRONIQUE TECHNIQUE

46 DATA CENTER

Retrouvez notre fil d'informations sur la sécurité et le stockage sur :
www.globalsecuritymag.fr
www.globalsecuritymag.com

mobility for business

Le salon de toutes les solutions mobiles pour les professionnels et leur environnement de travail

8ème édition

Demandez dès maintenant votre badge grauit avec le code promo : GSM4B

17 & 18 OCTOBRE 2018

PARIS - PORTE DE VERSAILLES

Renseignements : informations@mobility-for-business.com / Tel : +33 1 44 78 99 40

www.mobility-for-business.com

Platinum Sponsors

izOrder praxedo Solution Cloud de gestion d'interventions XPLORE

Avec

Global Security Mag THE SECURITY & STORAGE MAGAZINE

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

THEMA

18

RED TEAM

CONTENTS

01 **Édito :** Red Team : les équipes sécurité à l'épreuve du Feu
03 **Editorial :** Red Teams: security teams facing a trial by fire
09 Diary

10 NATIONAL POLICY
- **Cybermalveillance.gouv.fr launches the first section of its awareness kit**
By Jérôme Notin, Managing Director of the national assistance platform Cybermalveillance.gouv.fr

12 GDPR
- ***Notify a personal data breach: when, where, what, how?***
Interview with Matthieu Grall, Head of Technological Expertise Department, CNIL
By Marc Jacob and Emmanuelle Lamandé

16 LEGAL BRIEFING
- **Red Teaming: simulation services tackling real-world challenges**
By Olivier Iteanu, Avocat, Lecturer at the University of Paris I Sorbonne

18 THEMA - RED TEAM
- **Red Teams: think like an attacker!**
By Marc Jacob and Emmanuelle Lamandé
- **Red Teams and social engineering: win no matter what!**
By Marc Jacob and Emmanuelle Lamandé
- **Have I Been Pwned? – Yes you have!**
By Virgile Jarry, cybersecurity auditor at ACCEIS

40 TECHNICAL REVIEW
- **Large scale deployment of industrial IoT security**
By Quentin Heyler, Operational Security Expert for ERIUM

44 RAISING SECURITY AWARENESS
- **Security AWARENESS QUIZZ**
By Arnaud Soullié, Manager, and Charles Ibrahim, Consultant - Wavestone

46 DATA CENTER
- **"HDS" certification: the pill may be difficult to swallow for some operators**
By Marc Jacob and Emmanuelle Lamandé
- **Carrier neutral colocation housing and responsibility for data protection**
By Anthony Coquer, Security & Organization Department, Lexing Alain Bensoussan Avocats

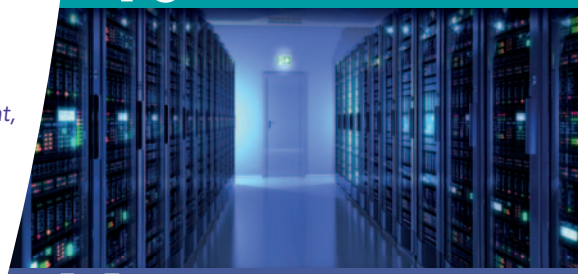
10 NATIONAL POLICY

12 GDPR

16 LEGAL BRIEFING

18 THEMA

40 TECHNICAL REVIEW



46 DATA CENTER

Keep up-to-date with the latest news on security and storage at:
www.globalsecuritymag.fr
www.globalsecuritymag.com

GSDAYS

LES JOURNÉES FRANCOPHONES DE LA SÉCURITÉ

11ème ÉDITION

9 AVRIL 2019

ESPACE SAINT-MARTIN - PARIS 3ème

Un cycle de conférences techniques, organisationnelles et juridiques

GS Days
LES JOURNÉES FRANCOPHONES DE LA SÉCURITÉ

AGENDA

AGENDA MIS À JOUR EN CONTINU SUR WWW.GLOBALSECURITYMAG.FR

JUILLET

30 juin - 1er juillet Paris
Nuit du Hack
www.nuitduhack.com

1er - 3 juillet - Berlin (Allemagne)
Security of Things World
www.securityofthingsworld.com

5 juillet - Londres (UK)
PCI London
www.e-crimecongress.org/event

11 juillet - Paris
CyberCercle
www.cybercercle.com

15 - 18 juillet - Rhode Island (USA)
DFRWS USA
www.dfrws.org/conferences/dfrws-usa-2018

17 - 19 juillet - Sarawak (Malaisie)
Critical Infrastructure Protection & Resilience Asia
http://cip-asia.com

25 - 27 juillet - Melbourne (Australie)
Security Expo
www.securityexpo.com.au

AOÛT

4 - 9 août - Las Vegas (USA)
Black Hat Briefings & Training Federal
www.blackhat.com

9 - 12 août - Las Vegas (USA)
DEFCON
www.defcon.org

16 - 18 août - Hô-Chi-Minh-Ville (Vietnam)
Secutech Vietnam
www.secutechvietnam.com/en

19 - 23 août - Santa Barbara (USA)
Crypto
https://crypto.iacr.org/2018

20 - 21 août - Sydney (Australie)
Gartner Security & Risk Management Summit
www.gartner.com/events/apac/security

SEPTEMBRE

5 - 7 septembre - Las Vegas (USA)
InterDrone
www.interdrone.com

11 - 14 septembre - La Haye (Pays-Bas)
Hardwear IO
https://hardwear.io/

17 - 19 septembre - New York (USA)
Global ID Summit
https://globalidsummit.iqpc.com/?utm_medium=portal&mac=IDGA_Events_Learn_Listing

18 septembre - Genval (Belgique)
DPO Forum
https://securityforum.pro/

18 septembre - Paris
Security Tuesday - ISSA France
www.securitytuesday.com

19 septembre - Londres (UK)
Securing The Law Firm
www.e-crimecongress.org/event

20 septembre - Toulouse
Cybersécurité et Territoires
www.cybercercle.com

24 septembre - Paris
Trophées de la sécurité
http://tropheesdelasecurite.fr

24 - 26 septembre - Porte de Versailles - Paris
Salons Solutions
www.salons-solutions.com

24 - 26 septembre - Marseille
Smart Security Week
www.smartsecurityweek.com

27 septembre - Paris
CyberCercle
www.cybercercle.com

4 juillet - Paris

Embarquez pour une soirée exceptionnelle de la sécurité 4.0

DU HACKING LAB AU SD-WAN SÉCURISÉ

Durant cet évènement organisé par Global Security Mag en partenariat avec IMS Networks et Fortinet, nous vous ferons découvrir comment vous protéger des dernières menaces et faire évoluer votre sécurité dans un écosystème innovant.
Grâce à la Fortinet Security Fabric, il est possible de mettre en place une protection globale et dynamique de votre environnement. IMS Networks, vous expliquera comment cet écosystème prend place dans une approche agile de Smart Secured Network.

FORTINET Global Security Mag ims NETWORKS

INTERVENANTS
Geoffrey Sombry, Channel Manager chez **Fortinet**
Mathieu Rigotto, Directeur du Pôle cybersécurité, **IMS Networks**
Soirée animée par Marc Brami, **GS Mag**

PROGRAMME
18h45 : Embarquement sur Le Signac
19h15 à 20h30 : Hacking Lab
20h30 à 23h : cocktail dînatoire et networking
Croisière sur Paris Seine

LIEU
Port d'embarquement et de débarquement : bâteau Le Signac
2 Port Debilly 75016 PARIS

Pour vous inscrire : https://linscription.com/soiréeGSMag4juillet-10751

CYBERMALVEILLANCE.GOUV.FR LANCE LE PREMIER VOLET DE SON KIT DE SENSIBILISATION

Par Jérôme Notin, Directeur général du dispositif national d'assistance Cybermalveillance.gouv.fr

Le dispositif national d'assistance aux victimes de cybermalveillance, Cybermalveillance.gouv.fr, vient de lancer le premier volet de son kit de sensibilisation à destination des entreprises, associations et collectivités. L'objectif de cette démarche est de sensibiliser les particuliers au travers du canal professionnel aux questions de sécurité du numérique, d'améliorer la prise de conscience des risques et de partager les bonnes pratiques.

Au regard de l'augmentation massive des attaques dans le monde numérique, le Gouvernement a décidé fin 2015 de mettre en place un dispositif capable d'apporter une assistance et de mener des actions de sensibilisation auprès des victimes d'actes de cybermalveillance. Incubé en 2016 par l'ANSSI et co-piloté avec le ministère de l'Intérieur, le dispositif cybermalveillance.gouv.fr a ainsi été lancé en 2017. Ce dispositif s'adresse aux publics n'étant traditionnellement pas concernés par les actions de l'ANSSI, à savoir les particuliers, les TPE, les PME et les ETI (hors OIV*), ainsi que les collectivités territoriales.

La plateforme cybermalveillance.gouv.fr offre ainsi aux victimes d'actes de cybermalveillance la possibilité de décrire, via un parcours « victimes », les menaces dont elles ont été l'objet, mais aussi de recevoir des conseils pratiques et de la sensibilisation. Elles peuvent également, le cas échéant, être mises en relation avec des prestataires de proximité en capacité de leur apporter une aide technique pour la remise en activité de leurs installations et matériels informatiques.

PLUS DE 1 500 PRESTATAIRES PRÊTS À APPORTER LEUR AIDE AUX VICTIMES

Cybermalveillance.gouv.fr s'inscrit, en effet, dans une démarche d'assistance de proximité : plus de 1 500 prestataires sont aujourd'hui référencés et peuvent apporter une aide concrète aux victimes sur l'ensemble du territoire national. Ces victimes n'ont le plus souvent pas de responsable de la sécurité informatique (pour les TPE-PME et les collectivités), et trop peu de culture de la sécurité numérique. La double action de sensibilisation et d'assistance est donc primordiale. Les prestataires informatiques sont des professionnels de toute taille, de l'entreprise unipersonnelle aux sociétés de services plus importantes. Lorsqu'ils postulent pour être référencés sur la plateforme, ils s'engagent via une charte à respecter les bonnes pratiques professionnelles et la confidentialité des données de leurs clients. Les prestataires qui portent assistance aux victimes s'engagent également à remonter vers le dispositif cybermalveillance.gouv.fr les données opérationnelles et les éléments techniques qui permettront au dispositif d'être à jour de l'état de la menace et des techniques utilisées par les attaquants.

De par sa vocation de guichet unique des victimes de cybermalveillance, le dispositif cybermalveillance.gouv.fr prend, en effet, également en charge une mission importante d'observatoire de la menace. Les actes de cybermalveillance font encore aujourd'hui l'objet de trop peu de plaintes et sont en sous-visibilité auprès de l'ensemble des services de l'État et du grand public. Les parcours renseignés par les victimes sur le site, ainsi que les rapports d'interventions et informations fournies par les prestataires de proximité vont donc permettre de mieux connaître et de faire connaître l'état de la menace actuelle en France, offrant ainsi une meilleure coordination de l'action publique.

Conscient des enjeux, le gouvernement a créé, pour porter ces missions, un Groupement d'Intérêt Public : le GIP ACYMA (actions contre la cybermalveillance). Ce GIP regroupe un collège étatique (rassemblant l'ANSSI, le Ministère de l'Intérieur, le Ministère de la Justice, le Ministère de l'Économie et des Finances et le secrétaire d'État en charge du numérique), un collège d'utilisateurs (regroupant principalement des associations de victimes, associations de consommateurs et associations professionnelles), un collège de prestataires de services informatiques, ainsi qu'un collège d'offreurs de solutions et de services. La forme juridique du GIP permet ainsi d'impliquer et de faire travailler ensemble le monde public et le monde privé. Les membres du GIP participent, par exemple, activement à la création de contenus de sensibilisation et aux actions de diffusion menées par les équipes du GIP.

UN KIT DE SENSIBILISATION À DISPOSITION DES ENTREPRISES, COLLECTIVITÉS, ASSOCIATIONS…

Un kit de sensibilisation a ainsi été créé pour être diffusé via le canal professionnel auprès des collaborateurs des entreprises et collectivités. Il a été lancé le 14 juin 2018 en présence de M. Mounir Mahjoubi, Secrétaire d'État en charge du numérique, et M. Guillaume Poupard, Président du GIP. Ce kit s'adresse au grand public par des contenus pédagogiques qui renseignent sur les types de menaces, les bonnes pratiques à adopter via une information de qualité et accessible.

Ce premier volet comprend un ensemble d'outils pédagogiques, axés sur quatre thèmes :

- Le hameçonnage (phishing) ;
- Les bonnes pratiques en matière de mots de passe ;
- Les bons usages des smartphones ;
- La distinction entre usages professionnels et personnels.

Chaque thématique est déclinée sous différents formats (infographies, vidéos, fiches pratiques, posters...) avec différents niveaux de sensibilisation.

Le kit a été créé afin d'être diffusé le plus largement possible au sein des entités (entreprises, collectivités, associations...). Les collaborateurs, sensibilisés via ce canal, pourront ainsi apprendre et mettre en place les bonnes pratiques de sécurité du numérique, tant pour leurs usages personnels que professionnels.
Les organisations qui participent à cette opération de sensibilisation contribuent de cette manière à améliorer l'hygiène informatique et la résilience de leurs collaborateurs, et par conséquence de l'organisation elle-même.

Les contenus sont mis à disposition sous une licence ouverte permettant son partage, son adaptation au sein des entreprises et sa réutilisation la plus large possible. Toutes les entreprises sont encouragées à télécharger son contenu et à lancer en interne les activités, ainsi que des campagnes de sensibilisation.

Pour télécharger le kit :
https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/.

---
* OIV : Opérateur d'Importance Vitale

NATIONAL POLICY

Cybermalveillance.gouv.fr launches the first section of its awareness kit

By Jérôme Notin, Managing Director of the national assistance platform Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr, the national assistance platform for malicious cyber-attack victims, has launched the first section of its awareness kit for businesses, associations and local authorities. The aim is to tackle the issue with the help of professional agencies, raise individuals awareness to digital security and risks and to share best practices.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

CNIL
Commission Nationale de l'Informatique et des Libertés

Notifier une violation de données personnelles : quand, où, quoi, comment ?

Interview de Matthieu Grall, Chef du service de l'expertise technologique, CNIL
Par Marc Jacob et Emmanuelle Lamandé

Depuis le 25 mai dernier, le règlement général sur la protection des données (RGPD) impose aux responsables de traitement de documenter a minima, en interne, chaque violation de données personnelles. Si celle-ci présente un risque pour les droits et libertés des personnes, elle devra de plus être notifiée à la CNIL, voire aussi aux personnes concernées, lorsque le risque est élevé. Matthieu Grall revient sur les principales obligations qui s'imposent en matière de violations de données et nous explique quand et comment notifier.

Global Security Mag : Qu'est-ce qu'une violation de données à caractère personnel ?

Matthieu Grall : Le RGPD définit dans son article 4 une violation de données comme étant « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ». Une violation de données se définit donc comme tout incident, d'origine interne ou externe, malveillante ou non, ayant comme conséquence une perte de disponibilité, d'intégrité ou de confidentialité de données personnelles.

Pour qu'il y ait violation, deux conditions doivent ainsi être réunies :
1. vous avez mis en œuvre un traitement de données personnelles ;
2. ces données ont fait l'objet d'une violation (perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou délibérée).

GS Mag : Quel cadre légal s'impose en matière de violations de données personnelles depuis l'entrée en application du RGPD ?

Matthieu Grall : L'entrée en application du RGPD, le 25 mai dernier, généralise l'obligation de notifier les violations de données personnelles à tous les responsables de traitement. Cette obligation s'inscrit dans le mouvement de responsabilisation des acteurs porté par le RGPD, qui leur demande d'assumer, auprès des autorités et des personnes concernées, l'impact potentiel induit par une violation et de justifier du déploiement de mesures visant à le limiter au maximum. Car au-delà des conséquences directes pour les responsables de traitement, de telles violations de données personnelles peuvent engendrer d'importants risques et dommages pour les personnes. Il est donc primordial de tout mettre en œuvre afin de limiter ces impacts.

L'obligation de notifier à la CNIL les violations de données à caractère personnel est prévue à l'article 33 du règlement général sur la protection des données [1]. Elle concerne tous les responsables de traitement de données à caractère personnel. Dans le cas où la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, l'article 34 du RGPD [2] impose de communiquer sur ces dernières aux personnes concernées.

DANS TOUS LES CAS, LA VIOLATION DE DONNÉES DOIT ÊTRE DOCUMENTÉE EN INTERNE

GS Mag : Concrètement, qu'est-ce qu'une entreprise doit faire en cas de violation de données ?

Matthieu Grall : Dans tous les cas, elle devra documenter en interne l'incident en déterminant :
- la nature de la violation ;
- si possible, les catégories et le nombre approximatif de personnes concernées par celle-ci ;
- les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- les conséquences probables de la violation de données ;
- les mesures prises ou qu'elle envisage de prendre pour éviter que cet incident ne se reproduise ou atténuer les éventuelles conséquences négatives.

Si l'incident constitue un risque au regard de la vie privée des personnes concernées, l'entreprise devra le notifier à la CNIL.
En cas de risque élevé, elle devra également le communiquer aux personnes concernées.
En cas de doute, mieux vaut notifier à la CNIL, qui indiquera à l'entreprise s'il est nécessaire ou non d'informer les personnes.

	Cas 1 : La violation n'engendre **pas de risques** sur les personnes	**Cas 2 :** La violation engendre un **risque** sur les personnes	**Cas 3 :** La violation engendre un **risque élevé** sur les personnes
Documentation en interne par l'organisme sous forme d'un **registre** interne de toutes les violations dont il est victime	X	X	X
Notification à l'autorité de contrôle, c'est-à-dire à la CNIL en France, si possible en 72 h	-	X	X
Communication aux personnes concernées dans les meilleurs délais, hors cas particuliers (mesures appropriées appliquées, risque réduit suffisamment, effort disproportionné)	-	-	X

GS Mag : Le RGPD prévoit-il certaines exceptions en ce domaine ?

Matthieu Grall : Certaines exceptions existent, relatives à l'obligation d'information des personnes concernées, néanmoins uniquement dans les cas suivants :

- des mesures appropriées ont été mises en œuvre et font en sorte que le risque ne devrait pas pouvoir se matérialiser. Par exemple, dans le cas d'une violation liée à la confidentialité, le chiffrement de données volées peut être reconnu comme approprié s'il repose sur un algorithme à l'état de l'art, que la clé utilisée n'a été compromise dans aucune violation et qu'elle a été générée de façon à ne pas pouvoir être trouvée via aucun moyen technologique existant ;
- des mesures appropriées ont été prises suite à la violation de telle sorte que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser. Par exemple, des mots de passe d'employés ont été subtilisés, mais n'ont pas été utilisés et ont été réinitialisés ;
- la communication aux personnes exigerait des efforts disproportionnés. Dans ce cas, il est plutôt recommandé de procéder à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

GDPR - CNIL

Notify a personal data breach: when, where, what, how?

Interview with Matthieu Grall, Head of Technological Expertise Department, CNIL
By Marc Jacob and Emmanuelle Lamandé

From 25 May this year, the General Data Protection Regulation (GDPR) requires data controllers to document, at least internally, each violation of personal data. Should this pose a risk to the rights and freedoms of natural persons, the CNIL must also be notified, and if the risk is high, individual data subjects informed as well. Matthieu Grall discusses the main obligations in terms of data breaches and explains when and how to notify.

SI LA VIOLATION PRÉSENTE UN RISQUE, ELLE DEVRA ÊTRE NOTIFIÉE DANS LES PLUS BREFS DÉLAIS

GS Mag : Dans quel délai une entreprise doit-elle notifier à la CNIL ?

Matthieu Grall : La notification doit être transmise à la CNIL dans les meilleurs délais à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes. Si vous ne pouvez pas fournir toutes les informations requises dans ce délai, car des investigations complémentaires sont nécessaires, vous pouvez procéder à une notification en deux temps :

1. une notification initiale dans les meilleurs délais à la suite de la constatation de la violation ;
2. puis, une notification complémentaire dans le délai de 72 heures si possible après la notification initiale ;
3. si le délai de 72 heures est dépassé, il conviendra d'expliquer, lors de votre notification, les motifs du retard.

En outre, dans le cas où l'organisme fait appel à un ou plusieurs sous-traitants impliqués dans la violation, ces derniers doivent prévenir dans les meilleurs délais le responsable de traitement après avoir pris connaissance de ladite violation, afin que ce dernier puisse remplir ses obligations.

UN TÉLÉSERVICE PERMET DE NOTIFIER LES VIOLATIONS DE DONNÉES AUPRÈS DE LA CNIL

GS Mag : De quelle manière peut-elle notifier une violation de données ?

Matthieu Grall : Pour notifier une violation de données, une entreprise peut utiliser le téléservice [3] disponible sur notre site à l'adresse suivante : https://notifications.cnil.fr/notifications/index. Via ce téléservice, les organismes touchés pourront transmettre les informations nécessaires à la notification de manière sécurisée.

GS Mag : Quels sont les éléments devant figurer dans une notification ?

Matthieu Grall : L'article 33 du RGPD décrit les informations que doit contenir *a minima* une notification à l'autorité de protection des données. Ces informations sont similaires à celles relatives à la documentation de la violation en interne évoquées précédemment :

FRANCE CYBER SECURITY

LABEL FRANCE CYBERSECURITY

Le Label France Cybersecurity est fier de présenter et de promouvoir aujourd'hui 89 offres labellisées, proposées par 72 entreprises nationales récompensées.

Retrouvez toutes les offres labellisées sur

www.francecybersecurity.com

- des informations sur la nature de la violation de données à caractère personnel ;
- les coordonnées de la personne à contacter afin d'obtenir plus d'informations sur la violation (en l'espèce, le DPO ou tout autre personne en charge) ;
- les conséquences probables de la violation pour les personnes impactées ;
- les mesures prises, ou à prendre, afin de remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif d'enregistrements concernés.

Les quatre premiers de ces points doivent être communiqués, en des termes clairs, simples et compréhensibles par tous, aux personnes concernées s'il est nécessaire d'informer ces dernières de la violation.

GS Mag : Une fois cette notification effectuée, que fera la CNIL ensuite ?

Matthieu Grall : Dès réception, la CNIL va instruire la notification. La procédure relative à la violation notifiée pourra être clôturée si la CNIL constate que :
- la violation ne porte pas atteinte aux données personnelles ou ne présente pas de risque pour les droits et libertés des personnes ;
- vous avez correctement informé les personnes concernées ;
- vous avez mis en place, préalablement à la violation, des mesures de protection appropriées.

La CNIL pourra vous imposer d'informer les personnes concernées si elle constate que :
- vous ne les avez pas correctement informées ;
- les mesures de protection que vous avez mises en place préalablement à la violation ne sont pas appropriées.

En outre, la CNIL souhaite apporter plusieurs choses aux organismes qui lui notifient des violations :
1. une aide dans la résolution de la violation ;
2. une alerte immédiate, publique ou ciblée, sans citer les cas notifiés, quand des attaques constatées pourraient rapidement concerner de nombreux autres organismes ;
3. un bilan annuel public.

UN PROCESSUS DE GESTION DES INCIDENTS DOIT ÊTRE MIS EN PLACE

GS Mag : Enfin, de manière plus générale, que recommandez-vous aux entreprises pour gérer leurs risques et incidents de sécurité ?

Matthieu Grall : L'incident de sécurité n'arrive pas qu'aux autres et, de plus en plus, celui-ci affecte des données personnelles devenant de facto une violation de données personnelles. Il est possible de gérer cette situation sereinement dès lors que l'on est préparé en amont. Ainsi, il apparaît essentiel que les organismes adaptent ou mettent en place un processus de gestion des incidents de sécurité dans le but d'être capables de les détecter, de les gérer et, le cas échéant, d'être en mesure de remplir leurs obligations légales.

Un processus classique de gestion des incidents en cinq étapes se base sur la norme ISO/IEC 27035 :
1. **Planifier et préparer :** il s'agit ici, en amont de la survenance d'un incident, de formaliser et de tester les procédures internes de gestion des incidents en créant un annuaire des parties impliquées et de ces procédures ;
2. **Détecter et signaler :** il faut être capable, en s'appuyant sur un travail de veille, de détecter un évènement de sécurité et de faire en sorte que les alertes soient traitées correctement afin d'être en mesure d'adopter la posture adéquate ;
3. **Évaluer et décider :** après avoir évalué les informations remontées et déterminé si l'évènement de sécurité est un incident avéré, il convient de qualifier l'incident, notamment dans le but de déterminer si ce dernier est une violation de données et de déterminer le risque engendré pour les personnes concernées. Dans le cas où la violation touche un traitement qui a fait l'objet d'une analyse d'impact relative à la protection des données (communément appelée PIA), l'analyse ainsi réalisée peut être utilisée pour faciliter l'estimation de la gravité de la violation en termes de risque ;
4. **Répondre :** il convient de déterminer et de mettre en place les mesures techniques ou organisationnelles permettant de résorber l'incident et de notifier la violation si cette dernière doit l'être, en fonction du risque engendré ;
5. **Tirer les enseignements :** le retour d'expérience est maintenant à capitaliser, afin d'empêcher que l'incident ne se reproduise. Les lacunes sécuritaires et organisationnelles sont identifiées et il convient de les corriger pour réduire le risque d'incident ou en atténuer les effets le cas échéant. Enfin, il convient également de revoir les risques et de mettre à jour les PIA en conséquence. ■■■

[1] https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article33
[2] https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article34
[3] https://notifications.cnil.fr/notifications/index

Pour en savoir plus : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
https://www.cnil.fr/sites/default/files/atoms/files/cnil-38e_rapport_annuel_2017.pdf

RED TEAM, UNE PRESTATION BIEN DE NOTRE ÉPOQUE

Par Olivier Iteanu, Avocat à la Cour, Chargé d'enseignement à l'Université de Paris I Sorbonne

Voilà un nouveau concept des pratiques cybersécuritaires qui vient poser un certain nombre de défis aux juristes : la Red Team ou le hacking éthique. Il s'agit en d'autres termes de reproduire des scénarii de cyberattaques réalistes pour tester la robustesse technique et organisationnelle d'une organisation. On pourrait aussi dire que la prestation Red Team est une cyberattaque dans toutes ses modalités, qui diffère de la cyberattaque traditionnelle à la fois par ses intentions et ses finalités. Mais a-t-on bien mesuré toutes les conséquences juridiques possibles ?

LA PRESTATION RED TEAM ET LE DROIT, POURQUOI PAS ?

Comme nous l'avons dit, la prestation Red Team diffère de la cyberattaque par ses intentions et finalités. Ainsi, si la cyberattaque tombe sous le coup de la Loi, c'est que son élément intentionnel est une partie intégrante du délit. En ce sens, pour reprendre les délits informatiques traditionnels, l'article 323-1 du Code pénal punit des peines maximales de deux ans d'emprisonnement et de 60 000 euros d'amende « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie… » d'un système d'information. Ainsi, cette violation du domicile électronique exige un accès intentionnel et on a envie de dire intentionnellement malveillant. Quant au maintien frauduleux, la jurisprudence a déjà retenu que l'accès pouvait être licite, par exemple par erreur, mais qu'ayant connaissance qu'il ne devait pas se trouver là où il se trouvait, l'individu s'étant maintenu est devenu délinquant. La Cour de cassation a ainsi retenu « que la seule découverte par O. L. de la présence d'un contrôle d'accès sur la page d'accueil [d'un site Internet] suffisait à établir que ce dernier avait conscience de son maintien irrégulier dans le système à l'insu et contre le gré de son propriétaire » [1]. L'article suivant du Code pénal qui vise les cas de virus informatique, bombes logiques, vers en tous genres, punit de 5 ans d'emprisonnement et de 150 000 euros d'amende, « le fait d'entraver ou de fausser le fonctionnement d'un système… », le choix des vocables utilisés par le législateur « entraver », « fausser » indiquant un fonctionnement non prévu par le propriétaire du système et provoqué par un acte intentionnellement malveillant. Ainsi donc, la prestation Red Team diffère manifestement par cette intention malveillante qui lui est étrangère. Mais la prestation Red Team diffère également d'une action illégale, par ses finalités. Il s'agit, par cet acte de hacking éthique, de tester les limites sécuritaires d'un système d'information. Il s'agit d'une finalité de sécurité. Or, le législateur français dans une Loi qui avait fait polémique pour d'autres raisons, la Loi de Programmation Militaire de fin 2013, avait justement introduit une exception à la commission de délits informatiques. Ainsi, dans un but de recherche, des chercheurs peuvent manipuler des virus informatiques, sans courir le risque de poursuites judiciaires. Mais la Loi, dans un article 323-3-1 du Code pénal glissé au milieu de la section « des atteintes aux systèmes de traitement automatisés de données », ajoute que les délits informatiques, notamment et principalement ceux que nous avons cités ci-avant, ne seront pas constitués si ces actes d'accès, de maintien, d'entrave du système sont réalisés pour un « motif légitime, notamment de recherche ou de sécurité informatique ». Oui, de sécurité informatique. Cela signifie bien sûr que pour l'équipe en charge de la prestation Red Team, ce motif légitime soit prouvable. Il le sera, par exemple, si un contrat a été conclu entre le prestataire et le propriétaire du système. On voit donc bien qu'il existe de nombreux motifs en droit, pour ne pas condamner par avance la prestation Red Team. Sa légalité est envisageable.

OUI, MAIS GARE AUX CONSÉQUENCES JURIDIQUES

Le problème de la prestation Red Team vient du fait que le système d'information n'est plus un tête-à-tête entre le prestataire et son client. Ce système renferme quantité d'autres intérêts. Qu'on se rappelle notamment l'obligation de notification d'une violation de

données personnelles, généralisée à tous par le Règlement UE 2016/679 dit RGPD, quand elle était jusqu'alors et depuis 14 ans réservée aux seuls fournisseurs de services de communications électroniques. Ainsi donc, l'article 33 du RGPD contraint le responsable de traitement de données personnelles à notifier une violation de données personnelles à la CNIL dans les meilleurs délais et si possible dans les 72 heures de la connaissance de la violation. Et le texte ajoute en son article suivant, que « lorsqu'une violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique… », le responsable de traitement doit communiquer l'existence et certaines modalités de cette violation à chacune des personnes concernées. On peut parler ici des salariés, des clients, des prospects ou même de simples contacts, c'est-à-dire de toutes les personnes physiques, et de leurs données bancaires ou données de santé par exemple. On voit bien au travers de cette disposition communautaire que la question de la sécurité est susceptible de concerner une quantité importante « d'autres personnes juridiques » que le seul propriétaire du système d'information et son prestataire. La chose est sérieuse, car le défaut de notification ou communication peut coûter en sanctions administratives jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires, soit le second niveau de sanction prévu par le RGPD. Le risque de la prestation Red Team est de porter atteinte aux droits et intérêts de ces « personnes concernées » sans même le vouloir, mais causant un préjudice qui peut engendrer des recours juridiques. L'autre difficulté est le partage désormais mondial de réseaux numériques ouverts. Internet n'est rien d'autres que des technologies qui permettent l'interopérabilité de quantité de réseaux jusqu'à des réseaux numériques télécoms plus traditionnels et mobiles. La conséquence de cette situation est que la cartographie des risques s'en est trouvée bouleversée. Nous devenons tous responsables les uns des autres. La défaillance de l'un peut résulter en un préjudice pour l'autre. Si une défaillance, une faille, a engendré une intrusion qui rebondit jusqu'à un second système d'information, la véritable cible de l'attaque, la première défaillance peut rendre juridiquement responsable. Bien sûr, la cybersécurité n'a pas encore basculé dans l'obligation de résultat, une obligation de résultat qui serait d'ailleurs absurde. Mais l'obligation de cybersécurité est tombée depuis belle lurette dans l'obligation de moyens renforcée. La prestation Red Team est à la fois la bénéficiaire de frénésie de mesures de sécurité en tous genres auxquelles ont recourt toutes les organisations, mais pourrait être aussi son maillon faible. Le recours à la prestation Red Team, n'est-ce pas faire prendre un risque dont on ne mesure pas tout à fait les conséquences ? On ne peut répondre de manière absolue à la question. Le RGPD, toujours lui, si symptomatique de notre époque et cette dérive, demande aux « controller » et « processor » de données personnelles de prendre des mesures de sécurité techniques et organisationnelles « appropriées ». Ainsi donc, ceux qui auront le projet de recourir à la prestation Red Team devront-ils faire cette évaluation des risques élémentaire et préalable, et orienter la prestation pour minimiser de tels risques. On ne peut ainsi recourir à la prestation Red Team de manière aveugle. Là encore, le contrat liant le prestataire à son client aura la mission d'encadrer à la fois le périmètre de la prestation, les mesures de contrôle et d'instaurer une procédure de sauvegarde en cas de crise.

Oui, la prestation de Red Team est tout à fait possible en principe et en droit. Mais son recours doit être encadré pour en limiter les risques juridiques. ■■■

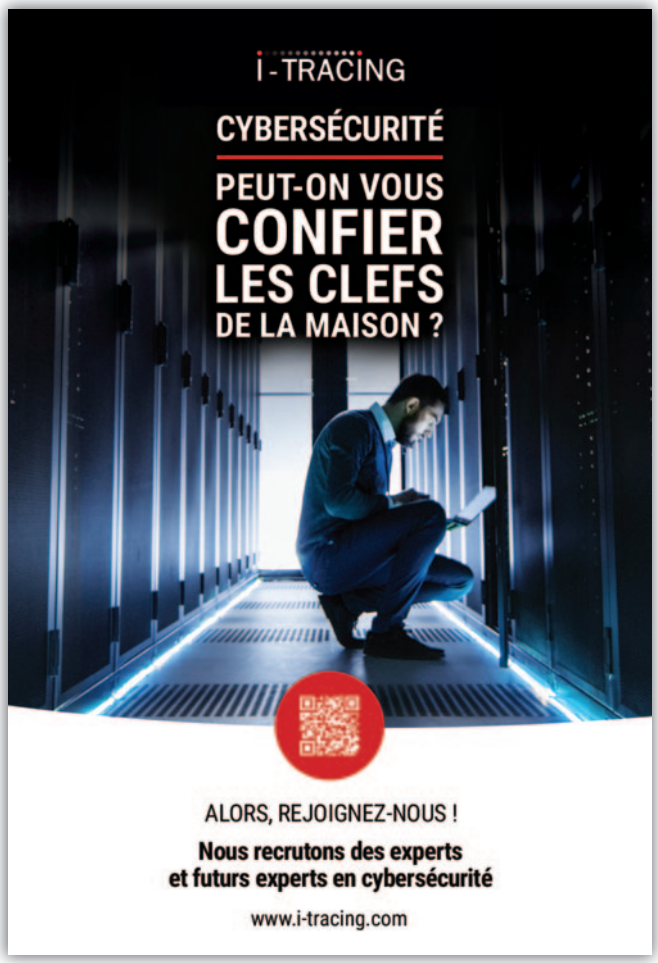
[1] Chambre Criminelle, Cour de cassation, 20 mai 2015 O.L.

LEGAL BRIEFING

Red Teaming: simulation services tackling real-world challenges

By Olivier Iteanu, Avocat à la Cour, Lecturer at the University of Paris I Sorbonne

Red Teaming or Ethical Hacking, which is a relatively recent approach to cybersecurity procedures, is raising a number of legal questions. The exercise consists of simulating realistic cyberattack scenarios to test the technical and operational robustness of an organisation. In other words a Red Team service can be seen as a fully-fledged cyberattack in every aspect, differing from a traditional cyberattack only in its intentions and purposes. But have all the potential legal implications been assessed?



Renaud Feil

Red Team : pensez comme un attaquant !

Par Marc Jacob et Emmanuelle Lamandé

Les Red Team voient leurs activités se décupler ces dernières années, au même titre que les menaces et les règlementations en matière de cybersécurité. Au travers de scénarios sur-mesure, définis au préalable avec le commanditaire, ces équipes spécialisées dans la mise à l'épreuve des SI vont tout faire pour « toucher là où ça fait mal » et trouver le maillon faible dans l'armure des entreprises… à l'instar du Talon d'Achille ! Pour nos deux experts, Renaud Feil, Synacktiv, et Vladimir Kolla, NetXP, outre l'aspect « démonstration », les Red Team aident avant tout les entreprises à tester et renforcer leur niveau de sécurité, physique comme logique, et à penser comme un attaquant !

Le concept de « Red Team », tel qu'il est aujourd'hui utilisé dans la sphère numérique, s'inspire en grande partie du monde militaire américain, qui avait pour pratique d'opposer des équipes d'assaillants (Red Team) à celles des défenseurs (Blue Team) lors d'exercices dédiés, en vue de renforcer leur résistance et leur résilience. Certains sous-traitants de l'armée américaine, comme IBM et SAIC, ou agences gouvernementales américaines, telles que la CIA, utilisent également ce type de démarche depuis de nombreuses années déjà **[1]**. Cette pratique s'est plus largement démocratisée aux États-Unis suite aux attentats du 11 septembre 2001. Afin de prévenir les défaillances ayant conduit à la catastrophe et de renforcer les systèmes de sécurité en place, le « *Defense Science Board* » a d'ailleurs recommandé, dans un rapport publié en 2003, le recours au « Red Teaming » **[2]**. Depuis, cette pratique gagne peu à peu du terrain dans les sphères publiques comme privées.

Objectif : détecter tous les défauts dans le bouclier d'une entreprise

Mais qu'est-ce qu'exactement une Red Team et en quoi consiste ses missions dans l'écosystème numérique ? Renaud Feil, Président et co-fondateur de Synacktiv, définit une Red Team comme « une équipe dédiée et spécialisée dans la mise à l'épreuve de la sécurité d'une organisation. Il s'agit le plus souvent d'une société externe qui essaie, à la demande de ses clients, de s'introduire dans les systèmes d'information comme le ferait un attaquant, afin de démontrer qu'il est possible d'y récupérer des données sensibles. Quelques grandes sociétés créent également aujourd'hui des petites équipes internes de Red Team ». Pour Vladimir Kolla, Responsable de la practice sécurité chez NetXP, il y a sûrement autant de définitions de Red Team que de Red Team elles-mêmes. Mais en général l'objectif est effectivement de réaliser une opération offensive avec des méthodes proches de celles de cybercriminels évolués ou d'agences gouvernementales, toutes proportions gardées, avec un but précis à atteindre. Bien que chaque cas soit spécifique, NetXP est principalement sollicité pour trois besoins aujourd'hui, explique-t-il :

- Tester les réactions d'un SOC dans le but de l'aider à s'améliorer ;
- Simuler une crise réelle, mais sans les impacts ;
- Réaliser une démonstration afin de convaincre en récupérant, par exemple, des données secrètes.

De manière générale, la mission d'une Red Team est de détecter des vulnérabilités critiques impactant l'ensemble du système d'information et la sécurité du patrimoine de l'organisation, souligne Renaud Feil. Elle va ensuite évaluer la robustesse du système en l'attaquant, et tester la réaction des équipes en charge de sa défense, souvent appelées « Blue Team ». La Red Team, tout au long de sa mission, va ainsi challenger, mettre en défaut et pousser la Blue Team à s'améliorer et à rester au niveau des attaquants. Son objectif sera donc de détecter tous les défauts, parfois subtils, dans l'armure des entreprises.

Red Team : une prestation qui suppose déjà une certaine maturité en SSI

« Toute société se posant la question de la sécurité de son système d'information peut en soi recourir à des tests de type Red Team », estime Renaud Feil. Synacktiv effectue d'ailleurs ce type de prestations dans tous les secteurs d'activité : des groupes industriels voulant éprouver la sécurité de leurs installations industrielles « connectées », des éditeurs de logiciels craignant le vol ou le piégeage de leurs codes sources, des laboratoires pharmaceutiques devant protéger leurs recherches, des cabinets de conseils et d'avocats qui sont au courant de projets confidentiels de leurs clients, etc. En revanche, Vladimir Kolla explique que « pour faire appel à ce type de prestation, il est impératif de disposer d'une grande maturité en sécurité des systèmes d'information. Vouloir réaliser une mission en Red Team sans les grands fondamentaux de la sécurité (politiques de sécurité, guides de durcissement par périmètre technique, sécurité périmétrique, défense en profondeur et détection des intrusions avec un

SOC) n'a pas de réel intérêt sauf, éventuellement, à vouloir démontrer concrètement une problématique de sécurité à sa direction, mais les grandes crises récentes de sécurité me semblent avoir déjà joué ce rôle. Pour cela, nous qualifions en amont le besoin avec le client et lui recommandons dans certains cas de faire plutôt un audit d'architecture et de configurations, plutôt que de se lancer dans une prestation onéreuse qui, certes, nous amusera mais n'aura pas de réel intérêt dans le contexte. »

Red Team : des experts qui n'ont pas peur de se salir les mains...

Entre un audit, un test d'intrusion et une Red Team, les approches sont effectivement distinctes, comme l'expliquent nos deux experts. En effet, « une Red Team est assez différente de nos tests d'intrusion où nous essayons de nous rapprocher d'une démarche d'audit, quasi exhaustive, sans s'arrêter une fois une ressource compromise », souligne Vladimir Kolla. Selon lui, « une Red Team est un test d'intrusion avec trois principales différences :

- La **démarche** n'est en rien exhaustive, mais plutôt **scénarisée** et, une fois le but atteint, nous arrêtons ;
- Le **périmètre** est bien **plus large**, quasiment sans limite. Nous pouvons fouiller des poubelles, pénétrer dans les locaux, poser des implants… même si parfois, certaines de ces actions sont simulées ou réalisées sous la surveillance d'une hiérarchie informée ;
- Nous sommes beaucoup moins contraints par le **temps**.

Un point commun avec les tests d'intrusion, mais sur lequel nous sommes beaucoup plus attentifs, réside dans la légalité de nos actions, car nous ne sommes pas des criminels et nous nous devons de respecter la loi, ainsi que l'éthique du métier. Cela se traduit par deux principales précautions :

- Nous évitons de compromettre des équipements personnels ;
- Nous évitons de compromettre des postes de travail de délégués du personnel, ce qui pourrait être interprété comme de l'espionnage mandaté par la direction. »

« Ce serait effectivement un abus de langage d'utiliser le terme « Red Team » pour une revue de la sécurité d'un code source ou un audit de configuration d'un serveur », complète Renaud Feil. « Dans son sens strict, la Red Team devrait simuler les méthodologies des attaquants, avec des approches de type boîte noire, démarrant avec un minimum d'informations sur la cible. Elle doit innover en testant des scenarios qui n'auraient pas été suffisamment pris en compte par les équipes sécurité. La Red Team doit tester la sécurité d'une organisation dans son ensemble (ou d'une partie significative), pas juste celle d'un serveur ou d'une application. De trop nombreuses organisations voient leur sécurité globale comme la moyenne de la sécurité de chaque composant pris individuellement. La Red Team permet d'illustrer le principe du maillon faible : ce sont en effet souvent les serveurs de test perdus au fond du système d'information, les vieilles applications « qui doivent bientôt être décommissionnées », ou encore des comptes utilisateurs « temporaires », qui permettent la compromission de l'ensemble.
Une autre valeur ajoutée des prestations Red Team réside dans leur pouvoir de démonstration, en particulier auprès de la direction. Cet exercice évalue de manière concrète ce qu'un groupe d'attaquants peut faire en un temps donné, avec tel budget. Et en donne la preuve. »

Des scénarios définis sur-mesure

Concrètement, comment se déroule une mission Red Team ? Vladimir Kolla explique « qu'une fois le besoin qualifié et tous les prérequis rédigés puis signés (convention, autorisation…), nous affinons les scénarios proposés en avant-vente, en prenant en compte certaines limites liées au contexte du client, nous nommons le responsable, composons l'équipe en fonction des compétences, puis démarrons la prestation.

Thema
RED TEAM

Red Teams: think like an attacker!
By Marc Jacob and Emmanuelle Lamandé

Red Teams have seen their activities grow in recent years, along with cybersecurity threats and regulations. These teams, specialized in the testing of IS, define with the client customised scenarios aiming to "hit where it hurts" and seek out the Achilles' Heel in enterprise armour. For our two experts, Renaud Feil, Synacktiv, and Vladimir Kolla, NetXP, in addition to providing an element of "proof", above all Red Teams help enterprises test and strengthen their level of security, both physical and logical, and to think like a attacker!

La première phase est une cartographie classique, allant de la collecte d'informations techniques à celle d'informations sociales sur l'entreprise ou les salariés. Cette cartographie permet ensuite de préciser les scénarios ou d'en obtenir de nouveaux, que nous proposons au client. S'ensuit une longue phase d'attaque, allant de quelques semaines à plusieurs mois, la plus discrète possible et pouvant évoluer suivant l'actualité de l'entreprise (évènements internes, départs, arrivées, fusions, nouveaux contrats…), l'actualité généraliste (soldes, élections…) et l'actualité sécurité (publication d'un code d'exploitation, d'une nouvelle vulnérabilité ou d'une nouvelle technique, découverte d'une vulnérabilité par NetXP…). A titre d'exemple, lors d'une opération, nous avions le contrôle d'un poste de travail très sécurisé depuis quelques jours. Le lundi matin à 9h, une vulnérabilité sur l'antivirus était publiée sur le forum FullDisclosure et à 11h nous avions élevé nos privilèges en toute discrétion. Le déroulement de la phase d'attaque est assez classique : cartographie, recherche de vulnérabilités, exploitation, progression, cartographie avec les nouveaux privilèges ou dans le nouveau périmètre, recherche de vulnérabilités… »

Renaud Feil considère, pour sa part, qu'il n'y a pas de prestation de Red Team « type », dans la mesure où tous les paramètres peuvent être adaptés en vue de répondre aux objectifs :

- Le périmètre : toute l'organisation ? Uniquement certaines filiales ? Uniquement certains sites physiques ?
- Planning : séquencement rapide avec une attaque intensive durant 2 semaines, ou attaque discrète étalée dans le temps sur 3 mois ?
- Les méthodologies autorisées : recherche d'information sur l'exposition Internet de l'organisation, tests d'intrusion externes sur tous les systèmes exposés sur Internet, attaques par phishing et spear-phishing (envoi d'une pièce jointe malveillante en vue de compromettre le poste de travail), social engineering, tests d'intrusion physiques sur un ou plusieurs sites, simulation de vols de portables ou téléphones mobiles pour accéder aux données, tests d'intrusion Wi-Fi, etc.
- Les trophées : quels sont les actifs que doit récupérer la Red Team afin que l'intrusion soit considérée comme réussie ?
- Niveau de coordination avec le commanditaire : quelle fréquence pour les points de suivi ? Il est recommandé de garder un contact régulier afin de s'assurer que les efforts d'intrusion vont dans le bon sens et d'être capable de s'arrêter quand on part sur une mauvaise piste.
- L'équipe devra être composée d'experts en intrusion d'un bon niveau,

HS2
Hervé Schauer Sécurité

Formation cybersécurité organisationnelle

PROGRAMME

Gouvernance de la sécurité

RSSI :
Formation RSSI
CISSP :
Préparation au CISSP
CISA :
Préparation au CISA
SECUHOMOL :
Homologation de la SSI
SECUCRISE :
Gestion de crise IT/SSI
EBIOS2010 :
EBIOS 2010 Risk Manager

Gouvernance de la sécurité avec les normes ISO270XX

ESS27 :
Essentiels ISO27001 & ISO27002
ISO27LA :
ISO27001 Lead Auditor
ISO27LI :
ISO27001 Lead Implementer
ISO27RM :
ISO27005 Risk Manager
ISO27004 :
ISO27004 / Indicateurs et tableaux de bord cybersécurité
ISO27035 :
ISO27035 / Gestion des incidents de sécurité

iStock
idcomm.fr

+33 644 014 072
www.hs2.fr
formations@hs2.fr

généralement un binôme, parfois plus. Elle doit, en outre, disposer d'une palette de compétences larges, ne sachant pas à l'avance sur quelles technologies elle va tomber !

L'exercice doit être bien cloisonné et « bordé » juridiquement

Quels que soient le contexte et les paramètres définis pour une telle mission, une chose est sûre : au niveau juridique, la Red Team « doit être bien bordée », comme l'explique Renaud Feil. « L'encadrement juridique et contractuel des tests Red Team est globalement similaire à celui des tests d'intrusion « classiques ». Mais il faut être attentif, malgré les préparatifs et tout l'encadrement possible, à certaines surprises. En effet, il peut arriver d'attaquer un système qui se révèle être mutualisé avec d'autres sociétés, ou par exemple appartenant à une filiale qui vient d'être vendue, mais dont le réseau est encore relié au réseau ciblé ! Depuis 6 ans que nous effectuons ce type de tests, les situations délicates se sont toujours facilement arrangées grâce à la bienveillance des acteurs impliqués. Mais je ne recommande pas ce type de tests dans des environnements où la priorité de chacun est plus de protéger ses arrières que son entreprise. Dans ces cas-là, mieux vaut réaliser un ersatz de Red Team sur un périmètre bien défini à l'avance.
Concernant la sécurité et la confidentialité, il est bien entendu important d'avoir confiance dans la Red Team, qui va potentiellement récupérer les données les plus sensibles de l'organisation. La sécurité des systèmes d'intrusion est ainsi primordiale, la probité des auditeurs aussi. Mais notons tout de même que, dans de nombreux scénarios, le commanditaire ne partage pas d'information avec le prestataire. Les informations sensibles récupérées pourraient très bien l'être de la même manière par une personne n'ayant signé aucun NDA ! »
Chez NetXP, complète Vladimir Kolla, « nous faisons signer une convention d'audit décrivant notre méthodologie, les rôles, les textes de lois, l'assurance, le périmètre, les limites… ainsi qu'une autorisation d'audit et quelques autres documents. Nous nous assurons aussi, de par notre expérience et connaissance des contextes, que le commanditaire est bien légitime et le conseillons sur les personnes à impliquer. Dans le doute, nous recommandons de faire appel à son service juridique. Supposons qu'un RSSI souhaite tester son SOC, nous pourrions recommander d'impliquer le responsable du SOC ou un niveau hiérarchique commun entre le SOC et le RSSI. »

Qu'elle soit ou non au fait des actions de la Red Team…

Quels sont d'ailleurs les acteurs qui doivent être complices de cette opération Red Team au sein de l'entreprise « testée » pour qu'une telle mission fonctionne, et existe tout court ? Nos deux experts sont d'accord sur le fait qu'a minima le donneur d'ordre est bien entendu au courant des actions menées par les Red Team, dans la mesure où il a la capacité juridique de s'engager pour ce type d'exercice. Le commanditaire doit, bien évidemment, avoir la légitimé suffisante et le mandat pour faire appel à ce type de prestation. Après tout dépend des clients, comme l'explique Renaud Feil, certains aiment bien prévenir les équipes techniques et la « Blue Team » afin qu'elles essaient de détecter et de bloquer les attaques. Cela permet de les faire participer activement à la prestation. D'autres préfèrent garder le secret, justement pour évaluer la capacité de leur SOC et des autres équipes à détecter les attaques sans avoir été prévenus. Effectivement, reprend Vladimir Kolla, dans certains cas, la Blue Team n'est pas au courant des opérations Red Team, et les découvre soit pendant son déroulement ou lors de la réunion de restitution. D'où l'importance d'impliquer le bon niveau hiérarchique et de bien cloisonner l'exercice afin d'éviter qu'il ne déborde. Il est, en outre, parfois possible d'avoir des complicités plus « atypiques », comme :

- Des salariés, dans certains cas de risque social ou tout simplement de manière à simuler une malveillance (se faisant compromettre volontairement, laissant une porte ouverte…) ;
- Des services de l'État ;
- Des entreprises ou personnes dont l'identité peut être usurpée pour un harponnage (spear phishing).

… la Blue Team devra défendre son camp !

Qu'elle soit ou non avertie de ce qui va se passer, le rôle de la Blue Team, en cas d'attaque, sera bien entendu de défendre son camp, expliquent à l'unisson nos deux spécialistes. L'objectif de la Blue Team est de « détecter les attaques réussies, mais aussi d'essayer de ralentir ou de bloquer la progression de l'attaquant », explique Renaud Feil. Elle doit, de plus, comprendre les défaillances et préparer les actions visant à améliorer progressivement ses capacités. Toutefois, son rôle ne s'arrête pas une fois l'exercice fini. On attend aussi d'une Blue Team une analyse de ce qui a fonctionné dans le dispositif de défense, et surtout de ce qu'il faut améliorer. Cet exercice peut être fait en collaboration avec la Red Team, qui présente la chronologie des attaques et son point de vue sur l'intrusion. C'est un travail primordial pour progresser. Quant à la direction, elle accueille souvent l'exercice avec un grand intérêt, dans la mesure où il lui permet de constater concrètement les résultats des investissements (ou du manque d'investissement) en sécurité informatique. Cependant, celle-ci doit faire preuve d'une certaine bienveillance envers ses équipes lors de la présentation des résultats, ou tout du moins un juste jugement. En effet, il est essentiel de faire la distinction entre une intrusion réussie avec beaucoup d'effort et une dose de chance pour les attaquants (à cause de quelques vulnérabilités isolées et difficiles à détecter), et une intrusion réussie de manière triviale sur des systèmes où aucun effort de sécurité n'est fait.

Tout est possible, tant que le commanditaire est d'accord

Effectivement, trouver le Talon d'Achille d'une entreprise n'est pas toujours chose aisée, même pour une Red Team, et nécessite parfois du temps et de l'effort. « Heureusement » pour les experts, les techniques et scénarios permettant de tenter une compromission logique et physique sont multiples. D'ailleurs, selon Renaud Feil, tous les scénarios sont possibles, tant qu'on est d'accord avec le commanditaire ! Toutefois, les techniques les plus classiques restent l'envoi d'e-mails piégés, comportant des macros Office malveillantes, des plug-ins de navigateurs piégés, des exploits récents pour certains des logiciels installés, etc. Dans d'autres sociétés, l'intrusion physique est triviale et la connexion d'un implant sur le réseau [3] permet d'établir un canal de communication entre le laboratoire de l'attaquant et le réseau interne ciblé. Enfin, autre technique classique : la compromission d'une application Web exposée sur Internet, permettant de compromettre plusieurs serveurs dans la DMZ et d'arriver à rebondir vers le réseau interne. Chez NetXP, Vladimir Kolla privilégie deux principaux vecteurs d'accès au système d'information d'une entreprise : l'hameçonnage (phishing) et l'intrusion physique (comme avec un faux entretien d'embauche ou le fait de suivre des employés après le déjeuner ou une pause cigarette) avec pose d'un implant. « Il nous est également arrivé de voler des équipements, mais parfois nous prouvons juste la faisabilité du vol et l'équipement nous est fourni. Cela nous évite de créer un traumatisme chez les salariés ciblés. Nos clients ayant majoritairement une bonne maturité sécurité, il est rare de pouvoir entrer directement par les ressources ou services exposés sur Internet, mais cela nous est arrivé, grâce à une cartographie précise et relancée régulièrement, permettant de détecter de nouveaux composants, par exemple en cours de déploiement et vulnérables. »

THEGREENBOW

Unique solution VPN pour des connexions sécurisées agréées

TheGreenBow VPN
Certifié CC EAL3+,
Qualifié standard,
agréé DR OTAN/UE

disponible pour tout équipement

Windows · Linux · MAC · Android · iOS

Logiciel VPN universel de confiance : connexion sécurisée avec toute passerelle VPN IPsec ou SSL, opérationnel sur réseau WiFi, 3G, ADSL et satellite, compatible toute IGC/PKI, compatible tout support d'authentification, token, carte à puce et OTP, Certifié CC EAL3+, Qualifié niveau standard, Agréé Diffusion Restreint OTAN et Union Européenne, habilité pour tous OIV.

www.thegreenbow.com

Le pire serait d'être démasqué !

Quel que soit le scénario choisi, une équipe Red Team se doit, pour parvenir à ses fins, de connaître de nombreux outils et techniques en fonction des technologies rencontrées. De son côté, Vladimir Kolla recommande d'utiliser en majorité des outils développés pour l'attaque en question, afin d'éviter toute signature connue. En effet, selon lui, le pire serait d'être démasqué et que les défenseurs se démotivent en comprenant que c'est un exercice. Effectivement, reprend Renaud Feil, en plus des outils publics, les prestations Red Team nécessitent de développer des outils sur mesure afin d'éviter une détection trop facile par les outils de sécurité. Un projet comme Oursin **[4]** permet par exemple de gérer l'envoi d'e-mails piégés à plusieurs destinataires et de récupérer les reverse-shell en provenance des postes de travail compromis. Par ailleurs, un système efficace de cassage des empreintes de mots de passe facilite grandement l'intrusion dans un temps limité **[5]**. En outre, disposer d'un grand nombre de bases de données de mots de passe compromis dans les fuites de données publiques permet souvent de démarrer les attaques avec quelques mots de passe valides chez des employés de la cible !

Réussir à s'infiltrer sans se faire prendre la main dans le sac relève parfois de l'exploit, et nécessite une véritable expertise en la matière. Toutefois, cette « intrusion autorisée » ne doit pas se faire au détriment de l'activité de l'entreprise. Outre son infiltration « incognito », la Red Team devra donc faire en sorte de ne pas impacter la production de l'entreprise lors de sa mission, du moins tant que ce n'est pas prévu et autorisé par le commanditaire. Selon Renaud Feil, une des règles pour ne pas impacter la production est de savoir ce qu'on fait sur un système compromis et, dans le doute, de ne pas prendre de risque ! À noter cependant que les exercices de type Red Team, du fait de leur caractère discret et reposant en grande partie sur des tests manuels, sont souvent moins risqués qu'un simple scan de vulnérabilités avec un outil automatisé générant une forte volumétrie sur du trafic malformé. Vladimir Kolla estime aussi « que, comme pour toute action technique, nous nous devons de maîtriser la portée de nos actions et les effets de bords induits. De plus, lors d'une mission Red Team, nous ne cherchons pas à faire de déni de service ou toute autre opération pouvant potentiellement impacter la disponibilité des équipements de production (ou alors, l'action sera réalisée en étroite collaboration avec le commanditaire dans le cas où nous désirons, par exemple, attirer l'attention des défenseurs en rendant volontairement un service indisponible). »

Les Red Team mettent en avant les vulnérabilités les plus critiques

D'une façon générale, Renaud Feil remarque que les tests d'intrusion de type Red Team permettent de mettre l'accent sur les vulnérabilités les plus graves, car souvent les plus faciles à exploiter dans un temps limité : manque de hardening du poste de travail des utilisateurs, mots de passe faibles ou réutilisés entre plusieurs systèmes, absence d'applications des quelques correctifs de sécurité vraiment critiques (ceux pour lesquels un exploit est disponible ou facile à développer), manque de cloisonnement du réseau interne, absence de contrôle d'accès au réseau de type NAC (Network Access Control), manque de personnel dédié pour filtrer les accès aux locaux, etc. De son côté, Vladimir Kolla note que les principales failles observées sont liées à des défauts de configuration, des manquements concernant le déploiement des correctifs de sécurité et de l'inattention (ou désintérêt) vis-à-vis des personnes environnantes ayant pourtant un comportement suspect. Une autre problématique réside dans l'asymétrie temporelle entre la publication de codes d'exploitation ou de correctifs (permettant d'en extraire la vulnérabilité) et le déploiement des correctifs.

Ces différentes failles de sécurité peuvent être exploitées de multiples façons et attirent diverses catégories d'acteurs malveillants, constatent nos experts. En effet, explique Renaud Feil, ces vulnérabilités classiques peuvent être exploitées par un concurrent (souvent via une officine d'intelligence économique peu scrupuleuse), par des mafias locales ou internationales, ou encore par des États trop curieux, etc. Effectivement, complète Vladimir Kolla, ces problématiques de sécurité peuvent être exploitées par des cybercriminels avancés réalisant des attaques ciblées, ou travaillant plutôt à l'opportunisme, des entreprises privées faisant du renseignement économique ou encore des agences gouvernementales… Toutefois, pour Renaud Feil, ce sont des attaques qui nécessitent quand même des efforts et une certaine préparation, elles sont donc plutôt le fait d'attaquants motivés. Inversement, certains vecteurs d'attaques restent compliqués à tester même en démarche Red Team, alors qu'ils pourraient l'être par un acteur malveillant : corruption d'un employé, compromission d'un sous-traitant, etc.

Afin d'éviter que ce type de scénarios ne se mette en application et une fois les vulnérabilités identifiées, les experts en sécurité vont aider l'entreprise testée à renforcer son niveau de sécurité. Ils vont, en ce sens, fournir dans leur rapport des recommandations détaillées à la fois techniques et organisationnelles permettant de corriger les vulnérabilités identifiées et expliquer les mesures pouvant être mises en œuvre pour rendre l'intrusion plus complexe. Par contre, rappelle Renaud Feil, « il est rare que ce soit la même équipe qui prépare les détails de mise en œuvre des projets de remédiations. La Red Team doit se concentrer sur le développement de son savoir-faire en intrusion afin de rester au niveau des attaquants ». De plus, pour Vladimir Kolla, « une Red Team n'a pas vocation à vérifier tous les périmètres, c'est plutôt ce que nous faisons lors de tests d'intrusion classiques où un de nos objectifs est de tenter de se rapprocher de l'exhaustivité en se basant sur des méthodologies détaillées et abordant quasiment tous les aspects d'un périmètre donné ».

Tout risque d'accident sur les personnes doit être écarté

Toutefois, avant de se lancer dans une démarche « Red Team », quelques points de vigilance s'imposent en amont, et les entreprises doivent mettre en œuvre un certain nombre de bonnes pratiques. Pour Vladimir Kolla, il est impératif, comme évoqué précédemment, de bien cadrer le sujet et d'impliquer les bons niveaux de hiérarchie, tout en définissant les limites de la mission. L'exemple classique est celui d'une compagnie aérienne ayant fait une campagne d'hameçonnage avec des promotions, dans le but de sensibiliser ses salariés. Mais certains d'entre eux se sont retournés contre l'entreprise afin de réellement bénéficier des réductions et ont obtenu gain de cause ! Renaud Feil considère, quant à lui, que le seul point véritablement important est de supprimer tout risque d'accident sur les personnes durant la réalisation de ces tests, ce qui passe par deux points de vigilance :

- L'expert arrête l'intrusion physique au moindre risque d'escalade violente. On ne cherche pas à fuir, on désamorce immédiatement la situation en sortant la lettre d'autorisation du management et on attend que la situation se règle pacifiquement, même si cela vient à faire échouer l'intrusion physique.
- On exclut du périmètre des tests tous les systèmes dont un dysfonctionnement peut avoir des conséquences pour des vies humaines (par exemple le central téléphonique dans une caserne de pompiers ou les systèmes de sécurité d'une installation industrielle). Ces systèmes seront testés avec les équipes du client et feront l'objet d'une coordination permanente afin de s'assurer que d'éventuels effets de bords soient détectés rapidement.

FORUM SÉCURITÉ @CLOUD

20 - 21 MARS 2019
PARIS - PORTE DE VERSAILLES

APPEL À COMMUNICATION

Vers un Cloud de Confiance ?

Enjeux - Analyses - Méthodologies

Keynotes-Tables rondes-Conférences

Informations :
c.moulin-schwartz@cherchemidi-expo.com

Avec :

ioT world

SOLUTIONS DATACENTER MANAGEMENT

CLOUD COMPUTING WORLD EXPO

www.iot-world.fr
www.datacenter-expo.com
www.cloudcomputing-world.com

Informations
@forumsecucloud

Chaque entreprise doit se mettre dans la peau d'un attaquant

De manière plus générale, Vladimir Kolla estime que chaque plan d'action visant à renforcer le niveau de sécurité d'une entreprise doit avant tout s'adapter à chaque cas particulier, les contextes étant tellement variés et spécifiques. Toutefois, un état des lieux sécurité sous la forme d'un audit d'architecture, voire organisationnel, peut déjà permettre à une entreprise d'identifier rapidement les écarts avec le niveau attendu et de bénéficier d'un plan d'action contextualisé. Sur un périmètre spécifique, un test d'intrusion peut également s'avérer pertinent. De son côté, Renaud Feil recommande aux entreprises de penser comme un attaquant : quelles sont mes informations véritablement critiques et comment ferait un attaquant pour les compromettre ? Il préconise également de miser sur la qualité des experts dans l'organisation afin de tirer le meilleur parti des systèmes existants. L'empilement de solutions de sécurité coûteuses ne sera, en effet, jamais une solution en cas de manque de compétence en interne.

Quoi qu'il en soit, il est certain que ce type de compétence et d'expertise sera de plus en plus recherché et prisé au sein des entreprises. D'ailleurs, selon nos experts, l'activité Red Team est promise à un bel avenir. Vladimir Kolla pense qu'avec l'avènement des SOC, cette prestation sera de plus en plus commune, même si cela restera tout de même une niche. « Nous voyons déjà des clients monter leur propre équipe mêlant tests d'intrusion classiques et Red Team. » Cependant, pour Renaud Feil, de nombreux facteurs vont rendre plus exigeant le travail des Red Team : la prise en compte croissante par les organisations des risques liés à la sécurité informatique, les budgets qui augmentent, la généralisation des SOC dans les grandes organisations, les efforts des éditeurs pour mieux sécuriser leurs produits, etc. « Une Red Team efficace va demander de plus en plus d'investissement pour pouvoir simuler les actions de groupes d'attaquants qui sont eux aussi de plus en plus perfectionnés. Je pense que nous assisterons à une escalade entre les quelques sociétés spécialisées en sécurité offensive et les grands groupes ayant la volonté et les moyens de se protéger. À côté de tout ça, les sociétés ayant peu de compétences et de moyens pour se défendre face à ces attaques ciblées ne pourront que constater, si elles en font l'exercice, leur incapacité à protéger leur activité », conclut-il. ■■■

[1] https://en.wikipedia.org/wiki/Red_team
[2] https://www.acq.osd.mil/dsb/reports/2000s/ADA430100.pdf
[3] Cf projet Houdini : https://www.synacktiv.com/ressources/synacktiv_houdini_plaquette.pdf
[4] Cf projet Oursin : https://www.synacktiv.com/ressources/synacktiv_oursin_plaquette.pdf
[5] Cf projet Kraqozorus : https://www.synacktiv.com/ressources/synacktiv_kraqozorus_plaquette.pdf

Red Teaming : le kit de piratage* de Tom Van de Wiele, F-Secure

1. Un presse-papiers, un gilet fluorescent, un casque ou tout autre vêtement correspondant à une stratégie réfléchie d'incursion dans les locaux de l'organisation. Ces accessoires doivent permettre de passer inaperçu, afin de réaliser une collecte approfondie d'informations ;
2. Des adaptateurs USB Ethernet, des adaptateurs Wi-Fi permettant l'extraction des données d'identification en liaison avec (4) ;
3. Des câbles Ethernet et autres câbles ;
4. Un implant réseau rogue permettant un accès ultérieur (contrôlé par F-Secure) au réseau interne, via internet ;
5. Proxmark3 (dessus) et carte d'accès RFID/NFC/Copieur/clôneur spécifique (dessous, en blanc) ;
6. « Rubberducky » personnalisé ou dispositif semblable permettant la sélection rapide de la charge utile et la saisie ou le forçage brutal du mot de passe en fonction de la cible ;
7. Mini-ordinateur « PocketCHIP » avec antennes Wi-Fi pour les attaques rogues de points d'accès Wi-Fi. Ce mini-ordinateur doit disposer d'outils permettant la collecte d'identifiants, le vol d'identifiants via Ethernet, ou l'exécution d'attaques de type man-in-the-middle. Batteries externes USB (non représentées) ;
8. Une sacoche (banane) avec laquelle se promener dans les locaux de l'entreprise visée. Les individus détenant des objets « utiles » ne sont pas considérés comme des intrus ;
9. Des pinces, tournevis et autres outils utilisés pour franchir certaines serrures, armoires (cartes d'accès, bandes de sauvegarde, clés, jetons d'accès, etc.) ;
10. Kit de serrurier avec visseuse automatique (non représentée), clés de frappes et clés de jiggler ;
11. Clavier pliable, à utiliser au besoin ;
12. Un trousseau/cordon comportant une clé, mais aussi une clé USB. Cette dernière doit contenir de faux documents attrayants, susceptibles d'être ouverts par l'individu qui découvrira le dit trousseau. Son ordinateur sera infecté et vous pourrez atteindre le réseau de l'entreprise (si l'ordinateur y est relié). Ces trousseaux doivent être déposées à l'intérieur du bâtiment dans la mesure du possible, ou aux abords extérieurs (parking ou hangar à vélos) dans le cadre d'un scénario d'ingénierie sociale « perte des clés » ;
13. Une *LAN Turtle* pour mener des attaques sur stock et des attaques réseau personnalisées ;
14. Module caméra infrarouge FLIR à raccorder à un smartphone pour photographier la chaleur latente laissée sur les claviers des employés. Les codes d'identification pourront être ainsi révélés, même si l'employé a dissimulé ses doigts pour les taper, et ce, durant environ une minute ;
15. Des enregistreurs de frappe USB avec Wi-Fi permettant de voir ce que tapent les employés tout en étant à l'extérieur du bâtiment ou via Internet, en combinaison avec un implant rogue (4).

*****https://fr.safeandsavvy.f-secure.com/2018/02/01/red-teaming-le-kit-de-tom/

Red Team & ingénierie sociale : à tous les coups l'on gagne !

Par Marc Jacob et Emmanuelle Lamandé

Au vu des différents retours d'expérience de nos experts Red Team, le niveau de sécurité global des entreprises testées apparaît en légère hausse et la prise de conscience s'opère, quant à elle, peu à peu. Toutefois, ce niveau reste encore largement insuffisant compte tenu des différents risques et techniques des attaquants. Que ce soit au niveau physique ou logique, les failles de sécurité assurent une intrusion réussie quasiment dans tous les cas. D'ailleurs, en la matière, l'ingénierie sociale reste le vecteur privilégié, et pour cause : à tous les coups l'on gagne !

Tom Van de Wiele, F-Secure

En regard des différentes missions effectuées en Red Team ces deux dernières années, nos experts sont quasiment tous unanimes : le niveau global de sécurité des entreprises testées est en légère hausse, bien que toujours insuffisant. Cependant, ce constat ne reflète pas le niveau de sécurité de l'ensemble des entreprises françaises, dans la mesure où celles qui font appel aux prestations de type Red Team sont déjà bien plus matures que la moyenne en matière de sécurité. Une maturité d'autant plus difficile à atteindre au vu de l'évolution du numérique et de la complexification croissante des organisations, comme l'explique Tom Van de Wiele, Principal Security Consultant, F-Secure. « Les entreprises sont des organisations complexes, qui créent sans cesse de nouveaux départements et font appel à de nouveaux prestataires de services, afin de conserver leur positionnement mondial ou simplement de rester compétitives. En matière de gestion du cyber risque, elles doivent prendre en compte de nouveaux paradigmes : le Cloud, les appareils appartenant aux employés et utilisés sur le lieu de travail (*Bring Your Own Device*), la dépendance à l'égard des prestataires informatiques, etc. C'est précisément via ces canaux que les cybercriminels parviennent sur votre réseau. Les attaquants connaissent la complexité des entreprises et peuvent s'en servir contre vous, en ciblant un employé ou un groupe d'employés. L'ingénierie sociale, associée à des astuces techniques intelligentes, ou au contraire très basiques, peuvent leur permettre de pénétrer sur le réseau. Les pirates vendent alors cet accès ou s'en servent eux-mêmes pour obtenir des informations qu'ils peuvent revendre : PII (*Personally Identifiable Information*), informations financières, propriété intellectuelle, etc. Ils peuvent également vouloir perturber certains services clés ou accéder à des fonds monétaires directs, comme des cartes de crédit, des bons, des licences, etc. »

Un niveau de sécurité en légère hausse...

Pour être efficiente, la gestion du cyber risque doit, selon Tom Van de Wiele, couvrir trois grands domaines : physique, social et cybernétique. Malheureusement, ce n'est encore que rarement le cas aujourd'hui. C'est là qu'entrent en jeu les simulations d'attaques destinées à renforcer votre protection : le Red Teaming. Dylan Dubief, Team Leader BU sécurité Offensive et Défensive, Openminded, souligne d'ailleurs, de son côté, le nouvel intérêt que portent des sociétés n'ayant, jusque-là, jamais fait appel à des prestataires d'audit en sécurité. « En effet, il y a encore quelques années, il était courant de rencontrer des clients qui n'avaient jamais réalisé de tests d'intrusion ou qui n'avaient pas connaissance de ce service en sécurité. Aujourd'hui, la communication sur le sujet est plus importante et la volonté de vouloir améliorer la sécurité de son organisation et de la challenger est devenue réelle et commune. En outre, et plus précisément au vu des résultats que nous pouvons constater durant nos missions, nous remarquons que les défauts de sécurité habituels (manquement dans les mises à jour, mots de passe en clair, etc.) se font de plus en plus rares. Les bons réflexes en matière de sécurité du SI deviennent une base commune. Cependant, et bien que cela soit une bonne chose, cela ne suffit pas. De nombreux vecteurs d'attaques sont encore laissés de côté, tels que la sécurité physique du SI ou bien la cryptographie. »

En effet, Adrien Guinault, Directeur technique chez XMCO, constate aussi une évolution du niveau de sécurité en demi-teinte. « D'un côté, les collaborateurs sont de plus en plus sensibilisés, les DSI ont compris que la sécurité devait être prise en compte et intégrée dans les projets stratégiques : ils allouent de plus en plus de budgets. Les réglementations, comme le RGPD ou PCI DSS…, et les services étatiques, tels que l'ANSSI, renforcent également cette tendance. Cela se traduit par une augmentation significative du nombre d'audits de sécurité et permet donc de constater une légère évolution du niveau de sécurité.

De l'autre côté, l'explosion du nombre d'applications Web, d'applications mobiles, de Web services, de prestataires SaaS, de nouvelles technologies (Docker, Kubernetes, etc.) et d'environnements Cloud (AWS, Azure) a accru le risque d'intrusion. En effet, la sécurité de ces environnements n'est pas toujours maîtrisée, ce qui induit de nouveaux risques. De son côté, le Patch Management reste toujours un problème qui peine à être adressé. Les dernières actualités (Drupal, Cisco, WebLogic) démontrent encore que les attaques opportunistes interviennent toujours plus rapidement, ce qui laisse très peu de temps aux DSI pour réagir (même si les nouvelles technologies permettent de réduire le temps d'application d'un correctif). Enfin, le vecteur d'intrusion qui permet d'obtenir le « RoI » le plus important reste l'humain au travers d'attaques de Spear Phishing (ciblé). »

... qui pousse les Red Team à peaufiner leurs techniques...

Walid Arnoult, Intrinsec

De toute manière, « dans le domaine de la sécurité informatique, c'est toujours le jeu du chat et de la souris : la recherche offensive fait avancer les techniques de défense et vice versa », remarque Walid Arnoult, Responsable Red Teaming chez Intrinsec. « Bien qu'il soit toujours possible de récupérer les trophées définis par le commanditaire de la prestation Red Team, nous avons cependant observé, au cours de ces dernières années, une amélioration de la sécurité applicative et une réduction de l'exposition des clients sur Internet. Cela rajoute donc du challenge à notre Red Team, qui doit user d'ingéniosité et de technique afin de réussir sa mission. Les techniques d'ingénierie sociale sont, en ce sens, couramment utilisées pour récupérer un accès au Système d'Information (SI) du client. En effet, l'humain est souvent le maillon faible de la chaîne de défense et donc une cible de choix pour un attaquant. Une fois sur le réseau interne, il convient d'user de discrétion afin de ne pas être détecté par la Blue Team, qui bénéficie désormais d'un outillage plus conséquent et plus perfectionné. L'arrivée des EDR (*Endpoint Detection and Response*) force, par exemple, la Red Team à améliorer sans cesse ses techniques et outils offensifs. Pour Intrinsec, avoir un SOC et un CERT en interne est donc fort appréciable, puisque des exercices de *Purple Teaming* peuvent être réalisés entre nos activités de défense et la Red Team, pour que chacun tire profit des expertises en attaque, défense et accompagnement des différentes équipes. Cela permet d'améliorer en permanence les schémas de détection, mais aussi l'efficacité des techniques d'intrusion et d'évasion de la Red Team, et ainsi de pouvoir faire face aux mécanismes de défense de nos clients. »

De son côté, Sysdream a réalisé plusieurs campagnes Red Team d'envergure ces deux dernières années pour des entreprises appartenant à différents secteurs d'activités, comme par exemple les médias, la presse, le secteur bancaire, ou encore industriel. « Des missions Red Team ont des enjeux parfois très sensibles, tels que la protection du droit d'auteur dans le secteur des médias, ou la sécurité des locaux et du système d'information dans le domaine de la presse (contexte des attaques terroristes) », explique Sophie Illès, Chargée d'Affaires Pôle Audit et Cyber-entrainement, Sysdream. « Ces campagnes se sont achevées par des succès importants, illustrant dans chaque cas plusieurs scénarios d'attaques et la compromission des systèmes d'information. Toutefois, le niveau global de sécurité de ces entreprises peut être considéré comme élevé. En règle générale, les missions Red Team sont demandées par des entreprises ayant déjà réalisé plusieurs tests d'intrusion (type pentest externe et/ou interne) sur leur système d'information, et qui sont donc plutôt matures sur les aspects de la sécurité. En revanche, le niveau de sécurité lié aux accès physiques et aux rapports humains est plutôt faible. Notre expérience nous montre, en effet, que les attaques par ingénierie sociale ont systématiquement permis à notre équipe Red Team d'accéder aux bureaux de l'entreprise. La sensibilisation des collaborateurs doit être un axe de travail prioritaire pour l'amélioration du niveau de sécurité de l'entreprise. » NES aussi mène régulièrement ce type d'audit, souligne Raphaël Illouz, PDG de NES. « Nous avons pu travailler avec différents secteurs d'activités et des entreprises allant de la PME à l'acteur du CAC40. Les retours de ces audits sont assez positifs dans l'ensemble et montrent globalement une hausse significative du niveau de sécurité des SI ciblés. Cela s'explique à deux niveaux : par sa nature, l'audit Red Team ne se limite pas à un périmètre restreint et se focalise plutôt sur un objectif précis. De ce fait, il est possible de mettre en relation les vulnérabilités/failles découvertes sur des périmètres d'ordinaire distincts, ce qui amplifie leur potentiel d'exploitation. Les failles recensées ont généralement un fort impact, aussi sont-elles traitées au plus vite par l'entreprise. Sans surprise, le deuxième élément à prendre en compte est la proportionnalité de l'investissement réalisé par la compagnie dans le domaine de la sécurité. Ainsi, le budget alloué, la qualité de la gouvernance en place et la prise de conscience des collaborateurs sont en adéquation directe avec les résultats. »

Thema
RED TEAM

Red Teams and social engineering: win no matter what!

By Marc Jacob and Emmanuelle Lamandé

In view of the feedback from our Red Team experts, there appears to be a small rise in the overall level of security and awareness of the enterprises tested. However the level is still largely insufficient given the range of risks and techniques used by attackers. Whether physical or logical, security breaches lead to a successful intrusion almost every time. In this area social engineering remains the preferred vector and for good reason: you can win no matter what!

... mais qui reste toujours insuffisant !

Lors de ses différentes missions, l'équipe Red Team de Synetis observe aussi de plus en plus fréquemment certaines améliorations quant au niveau de sécurité des entreprises. « Cela s'explique en particulier par la prise de conscience des Blue Team, la surmédiatisation des cyberattaques, l'adaptation de nouvelles directives (RGPD, par exemple) et l'accroissement de la sensibilisation au sein des écoles (formations dédiées à la cybersécurité). » L'équipe observe, de plus, une hausse des bonnes pratiques sur certains aspects, notamment l'adoption et le durcissement des réglages HTTPS, l'utilisation de Test de Turing (CAPTCHA) pour éviter la robotisation ou la modernisation des mécanismes d'authentification (fédération, SSO, SAML, OIDC). Certaines

entreprises ciblées sortent également du lot, avec une réactivité corrective à souligner et un renforcement poussé de la sécurité globale (PSSI, politique de mot de passe, orientation vers les Bug Bounty). A l'inverse, d'autres sont particulièrement vulnérables, avec un SI vieillissant, voire totalement obsolète : auquel cas une approche offensive sert surtout à illustrer aux métiers, par la démonstration, la criticité de certaines faiblesses via des cas concrets de sensibilisation récurrente. En outre, certaines vulnérabilités bien connues persistent souvent dans le temps chez bon nombre d'entreprises, tout comme certaines Blue Team ne maîtrisant pas l'intégralité de leurs systèmes d'information.

Yves Duchesne, ACCEIS

D'ailleurs, bien que la prise de conscience des risques commence à opérer au sein des organisations, Yves Duchesne, co-fondateur d'ACCEIS, estime de son côté que le niveau global de sécurité des entreprises testées reste clairement insuffisant. « Au gré des évènements récents (Wannacry, NotPetya, etc.), la menace cyber s'est un peu installée dans le paysage et une certaine prise de conscience a eu lieu chez les professionnels. Malgré tout, elle peine à se hisser à un niveau satisfaisant pour plusieurs raisons, à commencer par des questions de gouvernance. En effet, les professionnels de la gestion du risque peinent parfois à recueillir l'adhésion de leur direction, qui est pourtant essentielle et sans qui rien ne peut se faire efficacement. Il s'agit bien souvent de questions de budget, mais plus généralement de moyens mobilisés pour permettre au RSSI de travailler efficacement. L'autre principale raison est inhérente au facteur humain. Les utilisateurs du système d'information constituent un risque majeur et peuvent parfois faire preuve de beaucoup de réticence à appliquer les bonnes pratiques. Même lorsqu'un travail de sensibilisation est effectué, certains collaborateurs refusent tout simplement de suivre les consignes. Cet aspect est particulièrement prégnant lorsqu'il faut reconquérir la maîtrise du système d'information. La suppression des droits d'administration est parfois fort mal vécue, et l'intérêt manifeste de cette mesure est souvent mal compris. Par ailleurs, il faut garder en tête que les entreprises qui organisent des tests Red Team sont celles qui possèdent un niveau de maturité élevé en matière de gestion du risque. Aussi, cette perspective est assez vertigineuse et nous interroge très fortement sur le niveau de sécurité de celles qui n'ont pas cette maturité. »

Des collaborateurs encore trop naïfs et passifs, même en cas de suspicion...

Même si le niveau de sécurité des entreprises a légèrement augmenté, nous l'aurons compris au travers de ces différents retours d'expériences : il reste encore insuffisant et nos experts Red Team arrivent toujours au final à trouver, d'une manière ou d'une autre, là où le bât blesse ! Et contrairement à ce que l'on pourrait penser, ce ne sont pas toujours les failles logiques dans les systèmes d'information qui sont les plus faciles d'accès. La sécurité physique laisse elle aussi à désirer ! En effet, bien que des systèmes de protection soient généralement mis en place, certains salariés ou utilisateurs trouveront généralement des techniques pour se « simplifier » la tâche ! De plus, certains aspects font souvent l'objet d'une vigilance toute particulière en entreprise, alors que d'autres seront régulièrement négligés. L'exemple le plus significatif, évoqué par la plupart de nos experts, est celui de la sécurité physique mise en place à l'accueil, vs celle relative aux portes de services. Sans compter l'ingénierie sociale qui détient la palme d'or de tous les succès du Red Teaming !

« Notre retour d'expérience démontre effectivement que certaines failles de sécurité sont récurrentes », constate Sophie Illès. « Par exemple, nous avons souvent été confrontés au niveau des accueils à des SAS de sécurité hautement sécurisés, que l'on pourrait qualifier d'inviolables, tandis que les accès parking ou les accès des employés avaient un niveau de sécurité très faible. Les entreprises mettent souvent beaucoup de moyens sur la partie « accueil/visiteurs » de leurs locaux, au détriment parfois des accès secondaires.
La pratique de l'ingénierie sociale auprès du personnel présente également des failles humaines très récurrentes. Souvent, plus les prétextes sont gros, plus les collaborateurs y croient. Dans nos missions Red Team, contrairement à nos actions qui sont masquées et sous-jacentes, les consultants peuvent être très exposés aux collaborateurs. Le fait de discuter et de mettre en confiance les collaborateurs d'une société sur notre présence nous permet, par étapes, de tisser des liens et d'obtenir des informations ou des accès précieux. Aussi, une faille « humaine » fréquemment rencontrée est la non-action des collaborateurs ayant des doutes sur la légitimité de notre présence, mais qui ne vont pas pour autant donner l'alerte, souvent par manque d'information ou d'assurance sur les actions à mener en cas de suspicion d'intrusion. »

Souvent, on entre en entreprise comme dans un moulin

Dylan Dubief, Openminded

En France, nous manquons d'ailleurs cruellement de maturité en matière de sécurité physique, estime Dylan Dubief. Bien que les collaborateurs d'une société soient de plus en plus sensibilisés aux risques du social engineering, les intrusions plus poussées restent très simples à mettre en place et ont un taux de succès impressionnant. Pour lui, deux manquements sont particulièrement prépondérants en matière de sécurité physique, à commencer par les caméras de surveillance, qui ont majoritairement une fonction post-mortem, mais ne sont pas suffisamment contrôlées en temps réel. Ensuite, l'utilisation des badges reste problématique au sein des grandes structures : une fois à l'intérieur, personne ne vérifie lorsqu'un inconnu porte un badge ou non. De plus, nous avons encore trop tendance à penser qu'une personne à l'intérieur de locaux est légitime à y être, sans même savoir comment elle est parvenue jusqu'ici et ce qu'elle fait là.

« Nous retrouvons malheureusement presque systématiquement des défauts similaires entre plusieurs clients », constate Walid Arnoult. Cependant, il faut rappeler qu'à la différence d'un test d'intrusion, où le but est de rechercher des vulnérabilités sur un périmètre souvent contraint, le Red Teaming vise à entraîner les équipes de sécurité défensives (Blue Team) à la détection et à la réaction aux incidents sur un périmètre et une durée bien plus étendus. « Nous pouvons alors combiner différentes vulnérabilités pour élaborer un scénario d'intrusion efficient. Par exemple, le système de contrôle des autorisations

pour l'accès physique à l'entreprise repose souvent sur des technologies anciennes, en place depuis des décennies, et dont les frais d'installation et de mise à niveau sont très importants. C'est le cas de la technologie des cartes MIFARE dites « classic » (norme ISO 14443A), vulnérable aux attaques *nested* et *darkside*. Le scénario d'exploitation de notre Red Team est donc de récupérer un badge d'entrée d'un collaborateur via de l'ingénierie sociale et d'exploiter les défauts du badge pour le cloner, et ainsi s'introduire dans les locaux de l'entreprise. »

Le fumeur reste le meilleur ami de l'auditeur Red Team...

Adrien Guinault, XMCO

La sécurité physique demeure effectivement un problème majeur, déplore Adrien Guinault. Un phénomène certainement lié à la responsabilité de ce périmètre, qui incombe souvent aux services généraux et qui n'est donc pas maîtrisé par la DSI. La pauvreté des sécurités physiques MIFARE (absence de chiffrement, clefs par défaut, vulnérabilités connues) est, en effet, un point notable. Cependant, il est rarement nécessaire d'exploiter ces faiblesses techniques, puisque les modes d'organisation des entreprises (externalisation auprès de prestataires) facilitent les entrées/sorties des personnes… Il suffit encore trop souvent de suivre un employé qui entre le matin dans un bâtiment…

Pour Yves Duchesne, le meilleur ami de l'auditeur Red Team sur le plan physique reste sans conteste le fumeur, qui sort plusieurs fois par jour, souvent par une porte de service qu'il prend soin de bloquer en position ouverte. Les entreprises accordent souvent une grande importance à la sécurité de leur entrée principale, avec des portiques et du personnel d'accueil, mais certaines autres issues bénéficient d'une bien moindre protection, lorsqu'elle n'est pas tout simplement absente. A ce titre, l'installation de grooms et d'alertes sonores, lorsque la porte reste ouverte, permet de limiter les risques. Les contrôles d'accès à badges sont également un point parfois négligé. Leur installation est confiée à des entreprises d'électricité générale, qui n'ont pas forcément les compétences en interne pour faire les bons choix technologiques. Or, en la matière, de nombreux équipements présentent un niveau de sécurité beaucoup trop faible. Cloner un badge d'accès est souvent d'une facilité déconcertante.

De l'intrusion physique à la compromission logique, il n'y a qu'un pas...

Ces anomalies en matière de sécurité physique sont, en outre, majorées par les manquements en termes d'hygiène informatique, explique Yves Duchesne. « En la matière, plusieurs problèmes sont fréquents. En effet, on constate régulièrement un manque de contrôle d'accès au réseau, et il est souvent possible d'accéder au réseau d'exploitation en se branchant sur une prise réseau facilement accessible. Idem pour les réseaux sans fil, les points d'accès Wi-Fi sont souvent configurés en WPA en mode personnel, sans implémenter EAP. Mais une fois de plus, le facteur humain est le plus grand pourvoyeur de vulnérabilités. En la matière, on constate plusieurs types d'anomalies : mots de passe inscrits sur des post-it, tendance irrépressible à brancher des clés USB trouvées devant la machine à café et à ouvrir des pièces jointes douteuses, ou tout simplement absence de verrouillage de son poste durant la pause déjeuner ! Sans compter qu'une intrusion physique ne serait pas aussi problématique s'il n'était pas aussi aisé de brancher une *Rubber Ducky* sur un poste accessible par la suite… » « Le post-it est effectivement encore malheureusement d'actualité pour les approches offensives en interne, tout comme l'accès à des zones restreintes via un badge emprunté volontairement à un collègue le temps d'aller fumer une cigarette », constate l'équipe Red Team de Synetis. « Les clés USB de type *Rubber Ducky* sont également toujours aussi prolifiques au retour du déjeuner, surtout lorsqu'elles disposent d'un autocollant « RH » dessus. »

Raphaël Illouz, NES

« Lorsque les actifs de la société ciblée respectent l'état de l'art, l'attaquant va logiquement se tourner vers l'ingénierie sociale », explique Raphaël Illouz. « En effet, la médiatisation aujourd'hui omniprésente des failles de sécurité a incité les entreprises à mettre leurs machines à niveau, cependant il n'est pas aussi simple de sensibiliser efficacement l'ensemble de ses collaborateurs. Le phishing reste ainsi le vecteur d'attaque physique n°1. Un simple email imitant au mieux un haut responsable ou citant précisément les procédures avec lesquelles l'employé est familier fera souvent mouche. Tout dépendra logiquement des informations qu'il aura été possible de récolter en amont de l'attaque sans éveiller de soupçons.
Un second vecteur intéressant sera, lui, transverse aux niveaux physique et logique. Il s'agit effectivement de la clé USB malicieuse. Le pirate compte ici sur la curiosité de l'utilisateur quant au contenu d'une clé USB qui pourra recevoir un sticker avec un titre aguicheur. Dès l'ouverture de la clé, une charge malicieuse s'exécute permettant une prise de contrôle du poste au profit de l'attaquant qui a désormais un pied dans le réseau de l'entreprise. En outre, sur le plan purement logique, la fameuse injection SQL reste assez répandue et continue de justifier sa place au sommet des vulnérabilités Web. Il s'agit d'un véritable quick-win pour les attaquants. »

XSS, injection SQL, CSRF... : les Red Team ont l'embarras du choix

Dylan Dubief estime, pour sa part, que les défauts de sécurité logiques sont souvent les mêmes : exploitation d'une faille découverte il y a 3 ou 4 mois, fonctions ou services laissés à l'abandon ou encore des mesures de cryptographie prises sans compréhension et laissant un faux sentiment de sécurité… Bien que la sécurité des applications Web se soit nettement améliorée ces dernières années, Walid Arnoult constate, de son côté, qu'il existe toujours des défauts au niveau de la gestion des autorisations implémentées. « En fonction de la technologie cible, notre Red Team va chercher à exploiter des vulnérabilités permettant de l'exécution de code, pour ensuite obtenir un accès au SI du client. Enfin, la mise en place d'un système d'authentification double peut compliquer la tâche de la Red Team qui doit alors élaborer un scénario d'ingénierie sociale pour contourner celui-ci. » Pour Sophie Illès, les vulnérabilités logiques sont d'ailleurs globalement similaires à celles référencées lors d'un test d'intrusion : XSS, injection SQL, manque de protection du réseau, systèmes non mis à jour, etc. « La grande différence à prendre en compte durant la mission de Red

DEVENEZ QUELQU'UN DE RECHERCHÉ POUR CE QUE VOUS SAVEZ TROUVER

INVESTIGATION NUMÉRIQUE

- Inforensique : les bases d'une analyse post-mortem
- Inforensique avancée : industrialisez les enquêtes sur vos infrastructures"
- Rétro-ingéniérie de logiciels malfaisants

Dates et plan disponibles
Renseignements et inscriptions
par téléphone
+33 (0) 141 409 704
ou par courriel à :
formations-cyber@deloitte.fr

Conception : SIMPUB - 06 50 88 11 01 - Crédit photo : Shutterstock - Creations

www2.deloitte.com

Deloitte.

Team est le fait que notre équipe doit passer sous le radar de contrôle de l'entreprise, contrairement à un pentest classique, où toute la mission est bien planifiée et connue de l'équipe informatique en place dans l'entreprise. En mission Red Team, nos attaques doivent être complexes et préparées de manière à ne pas être repérées par la Blue Team. »

Pour Synetis, « les vulnérabilités les plus courantes sont très clairement :
- Les attaques de type XSS (*Cross Site Scripting*) ;
- Les attaques de type CSRF (*Cross Site Request Forgery*) ;
- Des faiblesses au niveau des mécanismes d'authentification (brute-force, énumérations, etc.) ;
- Des vulnérabilités liées au manque de mise à jour de services, distributions et de logiciels, ce qui laisse en général un grand nombre de points d'entrées exploitables pour les attaquants (*patch management*).

On retrouve ainsi régulièrement des énumérations d'utilisateurs, de clients, qui vont par la suite aboutir à des fuites de données personnelles, mais également à des transferts de points de fidélité, de « code de réduction » insécurisés par manque de cloisonnement des comptes ou de contrôle d'accès (vulnérabilités communément appelées IDOR - *Insecure Direct Object Reference*) ».

L'accès à un réseau interne engendre dans 9 cas sur 10 la compromission de l'AD

Effectivement, « les mots de passe (faibles ou par défaut) et l'absence de mises à jour des composants logiciels (serveur applicatif, CMS) constituent encore des vecteurs d'intrusion particulièrement utilisés et efficaces », explique Adrien Guinault. « Une fois sur le réseau interne, il suffit d'un défaut, voire de l'absence de cloisonnement (réseau à plat) et d'un seul serveur Windows vulnérable pour se déplacer latéralement jusqu'à obtenir un compte d'administration du domaine en mémoire. Les vieilles techniques fonctionnent donc toujours… L'accès à un réseau interne (physique ou au travers d'un cheval de Troie) engendre dans 9 cas sur 10 la compromission de l'Active Directory… En complément, les entreprises et collaborateurs utilisent de plus en plus d'outils SaaS et de partage (Jira, Github, Bitbucket, Pastebin like). Ainsi, il est de plus en plus fréquent de retrouver des données non protégées (code source, fichiers de configuration, mots de passe) laissées par un développeur ou un administrateur sur ce type de site Web. Des recherches sur ces canaux nous permettent souvent de trouver des points d'entrée… »

Enfin, le type de failles rencontrées, testées et le plus souvent exploitées dépend aussi du profil de l'attaquant. Il est effectivement essentiel, explique Tom Van de Wiele, de faire la distinction entre attaques opportunistes et attaques ciblées. « Les attaques ou intrusions opportunistes sont généralement le résultat d'une négligence ou simplement d'un manque de préparation aux scénarios les plus courants. Il peut s'agir d'un smartphone, d'un ordinateur portable ou d'une clé USB perdu(e), laissé(e) dans un taxi ou dans un train. Il peut aussi s'agir d'un ordinateur chez vous, sur un bureau, près d'une fenêtre côté rue, et dont un passant décide de s'emparer. Ces scénarios sont faciles à gérer, mais beaucoup d'entreprises présentent encore des faiblesses certaines sur ces contrôles de sécurité pourtant élémentaires. Parmi les attaques informatiques opportunistes, on retrouve les attaques aléatoires et massives auxquelles toutes les entreprises font face : les pirates scannent tout l'Internet à la recherche de vulnérabilités publiées, et susceptibles d'être exploitées.
À l'opposé, on retrouve les attaques ciblées, généralement opérées par des pirates ayant un but précis en tête. Dans 99% des cas, leur objectif est de générer de l'argent en dérobant des données ou en

Sophie Illès, Sysdream

perturbant un service. Pour parvenir à leurs fins, ils mènent le plus souvent des campagnes personnalisées d'ingénierie sociale et d'hameçonnage, en y associant parfois quelques intrusions physiques : ils attendent, par exemple, devant l'entrée latérale réservée aux fumeurs, en vue de pénétrer discrètement dans les locaux durant une pause ou le déjeuner. Dans d'autres cas, ils s'assoient juste à l'extérieur des locaux et utilisent leur ordinateur portable afin d'usurper des identifiants Wi-Fi, et d'accéder ainsi à des ressources. Mais quel que soit le mode opératoire choisi, les attaques ciblées fonctionnent et fonctionneront toujours…

Votre degré de protection peut être défini à partir de plusieurs questions : comment et à quelle vitesse vous pouvez détecter une attaque opportuniste ou ciblée ? Quels processus de confinement et d'éradication des menaces avez-vous mis en place ? En réalisant des tests de Red Teaming, avec les pires scénarios d'attaques, l'entreprise peut déjà repérer ses points faibles et être mieux préparée. Équipée des bonnes technologies de détection et d'intervention, armée d'outils capables de lutter contre les attaques les plus récentes, une entreprise ou une organisation pourra, en outre, gagner un temps précieux et éviter de nombreux problèmes juridiques, opérationnels ou liés à sa réputation », conclut-il. ■■■

Red Team : retour sur quelques anecdotes croustillantes !

Retour sur quelques anecdotes vécues par nos experts* et leurs équipes lors de missions Red Team, anonymisées bien sûr !

** Renaud Feil, Synacktiv, Vladimir Kolla, NetXP, Sophie Illès, Sysdream, Tom Van de Wiele, F-Secure, Dylan Dubief, Openminded, Adrien Guinault, XMCO, Yves Duchesne, ACCEIS, Walid Arnoult, Intrinsec, Raphaël Illouz, NES, et l'équipe Red Team de Synetis*

Plus c'est gros, mieux ça marche !

- « Comment se rendre de l'extérieur d'un bâtiment jusqu'au bureau du Directeur Marketing ? Après une longue phase de reconnaissance, nous avons choisi d'opérer durant un jour férié. Impossible de passer par l'entrée, sécurisée par badge et également par un SAS. Ayant observé des cyclistes contactant le PC Sécurité à l'interphone pour garer leurs vélos dans le parking, nous décidons de faire de même. Nous sommes en Vélib', sonnons à l'interphone du parking et prétextons un oubli de badge, et hop à l'intérieur ! Une fois dans le parking, nous en profitons pour fouiller les poubelles à la recherche de documents sensibles, puis nous cherchons le moyen d'accéder aux étages. L'ascenseur étant accessible uniquement avec badge, c'est via une porte portant la mention « Garder strictement fermée », qui était restée ouverte, que nous pénétrons dans l'escalier de secours. Cette voie nous amène directement au hall d'entrée du bâtiment et, par chance, la sortie débouche derrière le SAS de sécurité, donc nous évitons le contrôle d'identité ! C'est grâce au plan de sécurité incendie, obtenu durant la phase de reconnaissance, que notre équipe a pu emprunter les escaliers de secours et ainsi accéder aux étages. Nous sommes un jour férié, le premier étage est désert ! Un enregistreur de frappes physique est installé sur l'ordinateur portable du Directeur Marketing et des tests d'intrusion sont faits sur le réseau interne via un câble Ethernet.
  Le plus compliqué aura finalement été de revenir sur les lieux pour récupérer l'enregistreur de frappe qui avait été déposé. Nous empruntons le même chemin pour accéder aux étages, mais cette fois-ci, malgré l'heure du déjeuner, l'open space était rempli de collaborateurs. Ayant connaissance d'une coupure réseau antérieure, nous nous faisons passer pour la société de maintenance informatique, devant effectuer de simples vérifications de numéros de série sur les ordinateurs des collaborateurs, suite à cette coupure Internet. Ne se souciant de rien, ils nous laissent faire. Nous contrôlons quelques machines dans un premier temps pour ne pas éveiller les soupçons, pour arriver enfin à l'ordinateur du Directeur Marketing. L'affaire est dans le sac ! Notre équipe repart avec l'enregistreur qui a permis de récupérer les mots de passe vers l'ensemble des services sensibles de la société, nous permettant ainsi de compromettre son système d'information. »

- « J'arrive sur un plateau, je m'installe à un bureau vide, je me connecte, je scanne le réseau, tout le monde me regarde comme si je n'avais rien à faire là, personne ne dit rien. Je finis mes actions, et repars comme je suis venu. »

- « Comment réussir à pénétrer dans des bureaux et accéder au réseau d'une entreprise à partir de l'ordinateur de son directeur ? Tout simplement en se faisant passer pour un fournisseur, en entrant par la porte arrière de la cuisine, avec une boîte vide. »

- « Nous avons eu l'occasion de travailler dans des conditions très favorables lors d'un test Red Team, très confortablement installés dans une salle de réunion dont nous avons pu bénéficier toute la journée. Comment ? Tout simplement en utilisant le système de réservation de salles interne à notre client. Après avoir obtenu un premier accès, nous avons procédé à la réservation de cette salle, en usurpant l'identité d'un collaborateur, pour la journée entière, avec l'assurance que personne ne viendrait nous déranger. Et, en prime, avec la possibilité de faire preuve de culot si on tentait de nous déranger, en objectant fort légitimement que nous avions réservé cette salle.
  Nous avons appris par la suite que les administrateurs avaient remarqué l'intrusion informatique qui s'en était suivie et nous avaient cherchés toute la journée, sans succès. A leur décharge, il était très difficile de se douter que nous avions tout simplement réservé une salle de réunion. On doit, en outre, saluer leur très bon état d'esprit lorsqu'on le leur a expliqué. »

- « Lors d'une mission, pour laquelle un scénario d'ingénierie sociale par téléphone avait été élaboré, nous avons appelé des collaborateurs en nous faisant passer pour des techniciens du service informatique. Nous leur avons expliqué qu'une intervention était en cours, et qu'ils devaient nous communiquer leurs mots de passe par téléphone, afin qu'il n'y ait pas de problème avec leur sauvegarde. L'entreprise n'exposant pas de service d'authentification sur Internet, nous avons alors réalisé une intrusion physique afin d'obtenir un accès au SI avec les identifiants récupérés. Une fois sur place, nous avons alors été interpellés par une collaboratrice nous demandant si nous étions bien les techniciens ayant appelé la veille. Nous avons alors prétexté qu'elle avait sans doute dû avoir nos collègues en ligne, en nous empressant de changer de sujet. À notre grande surprise, la collaboratrice nous a alors avoué avoir fait une erreur concernant le mot de passe qu'elle avait communiqué par téléphone, et nous a tendu un papier avec le bon mot de passe. »

- « J'arrive dans une salle de réunion. Une personne rentre pour faire une réunion, et me dit que je n'ai pas réservé en me demandant de sortir. Puis, en sortant, me demande si je souhaite qu'on me réserve une autre salle. J'accepte bien entendu, et me retrouve dans une nouvelle salle de réunion qui a été réservée pour moi, avec accès au réseau interne. Tout cela sans nom, ni prénom, ni badge d'accès. »

- « Comment passer un appel téléphonique au RSSI depuis son propre bureau ? Notre équipe fait usage d'ingénierie sociale auprès du personnel d'accueil, nous indiquons avoir oublié notre badge dans notre bureau à l'étage. La procédure de l'accueil oblige à fournir une pièce d'identité pour pouvoir refaire un badge d'accès. Notre consultant Red Team indique n'avoir aucun papier sur lui, car en « pause cigarette », et présente sa carte bancaire pour montrer sa bonne foi. De fil en aiguille, il sympathise avec la personne de l'accueil autour de sujets divers. Après quelques minutes, nous obtenons un badge d'accès sans avoir fourni de pièce d'identité. Une fois installé dans le bureau du RSSI, notre consultant contacte par téléphone le commanditaire de la mission pour lui informer que la mission est accomplie. »

- « Se promener dans les sous-sols d'un Data Center après les heures de bureau et s'introduire par effraction dans la salle de l'ordinateur central est chose possible. Comment ? En reproduisant les empreintes digitales d'un employé sur les lecteurs de contrôle d'accès, à l'aide de papier hygiénique humide. »

- « Pour un client, nous sommes parvenus à pénétrer dans les locaux en accédant au parking, puis en ouvrant une porte de secours mal fermée menant sur une terrasse utilisée par l'ensemble de la société. Une fois sur la terrasse, nous avons joué le rôle d'un visiteur occupé au téléphone et avons regagné l'intérieur des locaux en suivant un employé… Depuis une salle de réunion, nous avons pu tranquillement réaliser notre intrusion logique et compromettre l'Active Directory en quelques heures. »

- « Autre exemple pour une grande organisation financière : démonter un distributeur de billets au beau milieu d'un centre commercial pendant que des centaines de personnes font tranquillement leurs achats autour de vous. Personne ne se méfie à cet instant, car vous portez l'arme cybernétique ultime : un gilet fluorescent. »

- « Je sème des clés USB à chaque étage de l'entreprise. Grâce à l'ouverture des pièces jointes attractives (« Augmentation Salaire 2018 », « Résultat_Entreprise_2017 »), je récupère nom utilisateur, mot de passe et IP de la machine, nom de machine, sur les différents services de l'entreprise. »

- « Une expérience que j'aime partager est celle d'un crochetage en plein jour et sous une caméra de surveillance. Ma mission était d'ouvrir une porte de service et de contrôler la réactivité des équipes de sécurité sur place, voir en combien de temps une personne passant à côté allait me poser des questions ou le temps d'intervention des personnes étant au contrôle des caméras. Visiblement, avoir une caisse à outils à côté de soi laisse penser qu'on est tout à fait légitime à ouvrir une porte de service. Après 1h à ouvrir et refermer la porte et à attendre l'intervention de quelqu'un, je suis reparti, personne ne semblait vouloir déranger le serrurier !
  Autre exemple intéressant : celui du cheval de Troie physique. Il s'agit d'un scénario que nous proposons en Red Team et qui, pour le moment, n'a jamais échoué. Il est question ici de revenir sur les premières intrusions de l'histoire et de reprendre la méthode des grecs, c'est-à-dire livrer un auditeur dissimulé dans un colis, une armoire, une grande imprimante, des poubelles vides, afin de le faire entrer sans passer par le poste de contrôle.
  Morale commune à ces histoires : plus une situation vous surprend (Que fait cette personne avec la porte ? Pourquoi recevons-nous une imprimante/Distributeur de café que nous n'avons pas commandé ?) et plus vous avez toutes les raisons de creuser la question : il vaut mieux déranger une personne légitime que de laisser passer un attaquant. »

Des vulnérabilités qui font toujours recette !

- « Lors d'une mission qui se déroulait jusque-là normalement et sans incident, nous avons identifié un serveur vulnérable à Heartbleed, qui nous a permis de récupérer la main sur celui-ci. Nous avons alors élevé nos privilèges et réalisé une reconnaissance passive. La prestation a cependant pris une tournure très différente quand nous avons analysé le trafic réseau. En effet, des serveurs en provenance de pays scandinaves étaient en train d'exploiter la vulnérabilité identifiée et potentiellement en phase de compromettre l'équipement. La prestation a donc été mise en pause pour qu'une investigation Forensics soit réalisée, afin d'évaluer la situation et de s'assurer qu'aucune information sensible n'avait été récupérée. »

- « Malgré le bruit médiatique des vulnérabilités Eternal Blue/Double Pulsar, nous avons pu trouver un grand nombre de serveurs vulnérables lors de missions offensives continues de type Red Team qui ont pu être exploitées, encore aujourd'hui, en 2018Q2. »

- « Il y a quelques mois, nous avons découvert une vulnérabilité de type injection de script sur un site statique, impliquant qu'aucune interaction avec l'utilisateur n'est prévue, et ne présentant donc qu'un intérêt moindre pour notre scénario. Nous nous sommes aperçus plus tard que le contenu de ce site statique était invoqué dans un recoin du portail client de l'entreprise présentant ainsi la vulnérabilité initiale sous un jour nouveau. Notre consultant est finalement parvenu à automatiser l'exécution de script lors d'opérations courantes initiées par les utilisateurs. Ainsi, bien que la base de données courante n'ait pu être atteinte, l'audit a démontré qu'il était possible de récupérer passivement des informations tout en contournant les sécurités en place. Pour contrer ce type de menace difficile à anticiper, il faudra se tourner vers le SOC qui lui pourrait détecter le flux illégitime... »

- « Pour une entreprise de la distribution, nous avons été amenés à tester la sécurité de l'encaissement et le niveau de détection des défenseurs. Nous avons simulé le vol d'une caisse en magasin pour l'analyser (inforensique) et en extraire des informations, comptes et firmware de terminaux de paiement. Par la suite, nous avons attaqué l'encaissement selon 3 axes :
  - Compromission d'une caisse avec injection d'un malware par un port USB et pilotage à distance ;
  - Injection d'une application malveillante dans les terminaux de paiement en remplaçant le firmware, présent sur les caisses, grâce encore à une clef USB ;
  - Compromission du poste d'un administrateur de l'encaissement par un harponnage (spear phishing). »

- « Dans le cadre d'une mission Red Team (sans intrusion physique), nous n'avions pas réussi à trouver un vecteur d'entrée sur le SI (échec du phishing, environnement logique peu important et intégralement en mode Cloud). Cependant, l'identification d'un dépôt appartenant à un développeur de la société et accessible publiquement a permis l'identification d'une clef AWS (utilisée pour l'automatisation et le déploiement complet de serveurs et d'applications) stockée dans un fichier de configuration. Cette clef possédant des droits d'administration sur l'environnement a donc permis d'atteindre aisément notre objectif final. »

- « La réalisation de campagne de spear phishing, afin de provoquer un point d'entrée contenant des pièces jointes malicieuses, reste un des vecteurs le plus prolifique lors d'approches offensives continues. Dans un cas précis, une personne-victime ayant ouvert le document infecté

AJOUTEZ LES NOUVELLES MÉTHODES DE DURCISSEMENT SYSTÈME À VOTRE ARSENAL

SÉCURISATION ET DÉFENSE

- Fondamentaux techniques de la SSI
- Sécurité des serveurs et applications web
- Sécurité Wifi
- Sécurisation des infrastructures Unix/Linux
- Sécurisation des infrastructures Windows
- Surveillance, détection et réponse aux incidents SSI

Dates et plan disponibles
Renseignements et inscriptions
par téléphone
+33 (0) 141 409 704
ou par courriel à :
formations-cyber@deloitte.fr

Conception : SIMPUB - 06 50 88 11 01 - Crédit photo : Shutterstock - Creations

www2.deloitte.com

Deloitte.

nous a répondu par email pour nous demander le renvoi du document, car elle n'a pas « réussi à l'ouvrir ». »

- « Après la compromission de serveurs de fichiers et partages réseau avec un compte à privilèges (mais non-administrateur), il nous a été possible d'accroître notre emprise sur le SI en s'emparant d'autres comptes et d'autres machines via une backdoor camouflée au sein d'un fichier PDF déposé volontairement sur ces partages. « Bulletin_de_salaire » ou « CV » sont des noms de fichiers particulièrement attractifs. »

- « Une société de conseil nous demande un exercice Red Team d'une vingtaine de jours-hommes. De nombreux CV piégés sont ouverts, transmis à plusieurs managers, y compris des membres de l'équipe informatique. Plusieurs postes de travail sont compromis, y compris ceux d'employés disposant de privilèges importants sur les systèmes. Nous progressons très rapidement sur un réseau peu cloisonné et en quelques jours l'ensemble du réseau interne est compromis. Nous démontrons que nous avons un accès total aux informations du CRM, aux projets clients, aux e-mails de la direction, etc. »

- « Lors de tests offensifs continus à l'encontre de cibles Web, dont les sources Git nous étaient disponibles (accès compromis précédemment), il a été possible de contourner à de multiples reprises les « patchs », « fix » et corrections que les développeurs mettaient en place en temps réel. Plusieurs jours de compromissions répétées se sont ainsi déroulés avant que le Git ne soit renforcé. »

- « Abus de confiance toléré : dans le cadre d'une approche offensive Red Team à l'encontre de cibles Web, un hameçonnage du RSSI lui-même a été réalisé par nos soins, en vue d'émettre une requête depuis le réseau corporate (filtrage basé sur l'IP corporate). Cette requête permettait de faire fuiter des fichiers hautement critiques sur un site e-commerce, uniquement si elle émanait de l'intérieur. »

- « Nous nous sommes introduits dans les locaux d'une entreprise et avons trouvé accès au réseau interne via un câble Ethernet. Notre équipe utilise la récente vulnérabilité MS17-010 de Microsoft pour attaquer le réseau de l'entreprise, et prendre le contrôle des postes non mis-à-jour. Les outils de sécurité interne lèvent alors une alerte concernant une compromission par le ver Wannacry, qui lui aussi, exploite cette vulnérabilité. En moins de 15 minutes après le début de l'attaque, la Blue Team arrive dans l'étage où nous nous étions installés, en criant aux collaborateurs « Ouvrez un terminal, tapez ipconfig et dites-nous qui a l'adresse IP qui finit en 57 !!!!! ». Nous n'avons tout simplement pas répondu à l'appel de la Blue Team, et aurions pu quitter les locaux sans être inquiétés. Après quelques minutes, notre Red Team s'est désignée, afin d'éviter un trouble trop important auprès des collaborateurs. »

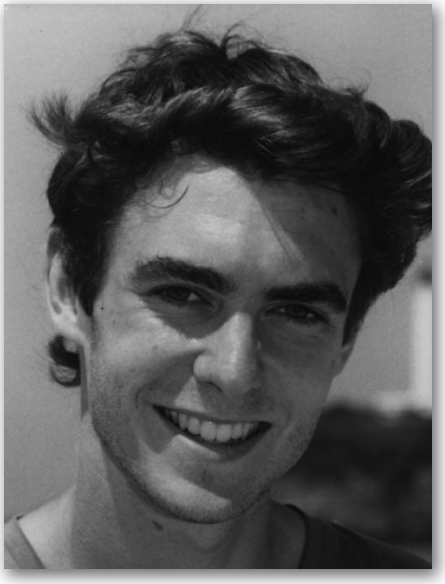
- « Un groupe français nous demande de démontrer qu'il est possible d'accéder à des données confidentielles en une cinquantaine de jours-hommes. Nous identifions un mot de passe faible sur un progiciel de gestion exposé sur Internet, puis plusieurs vulnérabilités accessibles après authentification qui nous permettent de rebondir vers plusieurs DMZ et finalement vers le réseau interne. Un administrateur du serveur de gestion se rend compte de l'intrusion, modifie le mot de passe faible et applique le patch pour une première vulnérabilité, mais ne prévient ni le SOC ni le CERT de sa société. En l'absence d'investigation plus poussée sur notre intrusion, personne ne s'est rendu compte que nous avons compromis d'autres comptes utilisateurs et identifié d'autres vulnérabilités, nous permettant de revenir sur les DMZ. Nous continuons notre intrusion jusqu'aux trophées. La liste des projets de fusion-acquisition que nous présentons, anonymisée certes, fait frémir la direction. »

Une lueur d'espoir pour la défense ?

- « Dans un contexte très sensible, nous avions pour objectif d'évaluer et de faire progresser le SOC, via la compromission de postes de salariés par un harponnage (spear phishing), mais aussi l'intrusion dans les locaux par la ruse et la pose d'un implant permettant la poursuite de l'attaque. Le bilan fut entre autres une amélioration de l'organisation, de la communication (dans l'équipe des défenseurs), de leurs outils et procédures, de la mise en place d'un interlocuteur privilégié par équipe et de la correction de vulnérabilités exploitées. »

- « Une mission Red Team nous a permis d'exploiter tous les vecteurs possibles pour nous introduire sur le réseau interne de l'entreprise ciblée : clef USB piégée, emails de phishing ciblés à des employés, intrusion physique, intrusion logique au travers de serveurs applicatifs exposés et mal configurés. Ce fut un bon cas d'école, mais cet audit a permis au client de sensibiliser l'ensemble de ses collaborateurs sur la base d'exemples concrets. »

- « Un dernier exemple pour donner espoir à la défense :-) Un grand groupe industriel nous demande de compromettre depuis Internet des sites industriels sensibles en cinquante jours-hommes. Malgré nos efforts et la compromission de plusieurs systèmes exposés sur Internet, nous n'arrivons pas à identifier comment accéder aux réseaux industriels qui semblent correctement filtrés et difficiles à trouver en aveugle. Plusieurs pistes que nous pensions intéressantes aboutissent finalement à des impasses et le commanditaire ne veut pas nous donner d'indication pour nous faire progresser plus vite. Nous présentons finalement les résultats des intrusions et confirmons qu'il n'est pas trivial pour un attaquant disposant du même budget et du même niveau d'information (et de compétence) que nous de compromettre les sites industriels depuis Internet. » ■■■



Have I Been Pwned ? – Yes you have !

Par Virgile Jarry, auditeur en cybersécurité chez ACCEIS

Une phase s'avère particulièrement importante lors d'un audit Red Team : la recherche d'informations blanches et des listes de mots de passe ayant fuités de services tiers. Toutefois, cette étape peut s'avérer particulièrement fastidieuse et longue selon la quantité de données à traiter. Pour simplifier cette démarche et améliorer l'efficacité de ses tests Red Team, ACCEIS a développé un outil dédié à la recherche d'identifiants dans des bases de mots de passe : LeakScraper.

Lors d'un audit Red Team, une phase importante est celle de la recherche d'informations blanches (phase qualifiée d'OSINT pour OpenSource INTelligence). Parmi les informations publiques dont des attaquants disposeraient se trouvent des listes de mots de passe ayant fuités de services tiers, tels que Dropbox, Myspace, LinkedIn ou encore Tumblr. Ces listes de mots de passe proviennent d'autres attaquants ayant compromis ces services et récupéré, depuis leurs bases de données, la liste des comptes utilisateurs, ainsi que leurs mots de passe (ou en tout cas, le hash de leurs mots de passe). Il suffit de se rendre sur le site *haveIBeenPwned.com* pour se rendre compte de la quantité de mots de passe ayant fuités sur Internet.

Rechercher parmi ces fuites de données peut s'avérer particulièrement fastidieux et long en fonction de la quantité de données. Il est pourtant important de ne négliger aucun élément disponible dans ces données, car le moindre mot de passe valide peut servir de point d'entrée pour une attaque très efficace, qui n'aurait pas pu avoir lieu sinon. Chercher des couples d'identifiants valides sur des applicatifs d'une cible à partir de mots de passe déjà utilisés auparavant par les mêmes personnes (sur d'autres services tiers) s'appelle le *credential stuffing*. Un couple identifiant/mot de passe fonctionnant sur un applicatif particulier est très intéressant pour des attaquants, car les applications protègent généralement mieux leur périmètre que leurs fonctionnalités internes. En un mot comme en cent : il existe beaucoup plus de vulnérabilités applicatives nécessitant une authentification préalable que de vulnérabilités n'en nécessitant pas.

Leak scraping for fun and profit

Afin d'améliorer l'efficacité de ses tests Red Team, ACCEIS a développé un outil dédié à la recherche d'identifiants dans des bases de mots de passe (que l'on appellera des leaks). L'objectif est de partir des leaks déjà à disposition (plus de 200GB de fichiers texte) et de les indexer au sein d'une base de données que l'on puisse utiliser facilement pour obtenir, le plus rapidement possible, la liste des mots de passe dont les employés d'une entreprise sont susceptibles de se servir.

Description des besoins

Toutefois, l'outil doit remplir certaines fonctionnalités et respecter des conditions pour être pertinent :

- La fonctionnalité principale de l'outil est d'obtenir la liste des identifiants associés à un domaine précis. Par exemple, l'utilisateur entre le nom « microsoft.com » et obtient la liste des identifiants de personnes disposant d'une adresse email en « @microsoft.com » ;
- Il doit être facile d'ajouter de nouvelles données (de nouveaux leaks) sans que cela soit une opération trop longue ;
- La vitesse de recherche dans la base est la statistique à prioriser ;
- L'espace de stockage utilisé par l'outil n'est pas jugé comme étant une ressource limitée. L'outil va, en effet, créer des index en base et gérer un volume de données plus important que ce que représentent les leaks eux-mêmes. A choisir entre la vitesse d'exécution et l'espace de stockage, nous préférerons la rapidité d'exécution, dans une optique de compromis temps-mémoire.

Uniformisation des leaks

Le premier problème qui se pose quand on souhaite travailler sur des leaks réside dans la diversité des formats utilisés. Chaque leak présente ses données sous une forme différente, et contient des entrées inutilisables. En effet, les leaks contiennent énormément de lignes sans mot de passe, sans email, ou avec un email invalide. Certaines lignes sont, quant à elles, parfois obfusquées ; d'autres ne respectent pas le format utilisé dans le reste du fichier, etc. Si l'on souhaite intégrer toutes les données exploitables dans une base unique, il va falloir nettoyer tout ça ! Un point très important malgré tout est que nous ne souhaitons pas perdre la moindre information des leaks initiaux, même s'ils paraissent inexploitables. Il nous faut

donc un premier outil capable d'extraire les informations pertinentes d'un leak et de les transcrire dans un format « universel ». Le format choisi est le suivant : « email:hash:plain ». L'email est une donnée indispensable, contrairement au hash et au plain (mot de passe en clair), l'un des deux est suffisant pour rendre la ligne pertinente.

L'outil d'uniformisation des leaks ne peut, en revanche, deviner lui-même le format que le leak utilise initialement. Il faut donc demander à l'utilisateur de décrire une ligne typique du fichier initial, par exemple à l'aide d'une expression rationnelle passée en argument à l'outil. Ainsi, si plusieurs formats cohabitent au sein du même leak, il est possible de recommencer l'opération pour les extraire les uns après les autres.

Pour décrire une ligne d'un leak lors de son nettoyage, l'utilisateur devra préciser où se trouve l'email, le hash et/ou le plain. Cela peut se faire à travers des groupes capturants nommés, fonctionnalité nativement disponible lorsqu'on utilise des expressions rationnelles.

Prenons un exemple : l'utilisateur dispose d'un fichier CSV contenant les colonnes suivantes :
id,timep,email,status,gender,country,username,birthday,password

L'utilisateur pourra fournir l'expression rationnelle suivante :
(?:.+?,){2}(?P<email>.+?),(?:.+?,){5}(?P<plain>.*)

Cela aura pour effet de retourner toutes les lignes respectant le format CSV identifié, tout en extrayant l'email et le mot de passe de chaque ligne à travers les groupes capturants nommés « email » et « plain ». Le résultat à tout cela est un outil dédié à l'uniformisation de leaks fonctionnel et efficace.

Thema
RED TEAM

Have I Been Pwned? - Yes you have!
By Virgile Jarry, cybersecurity auditor at ACCEIS

One phase is particularly important during a Red Team audit: the search for "white market" information and password lists that have leaked from third-party services. Nonetheless, depending on the amount of data to be processed, this phase can be particularly tedious and time consuming. To simplify this process and improve the efficiency of its Red Team tests, ACCEIS has developed a tool dedicated to finding usernames in password databases: LeakScraper.

```
Perf. tunning : 1 threads / 4096 buffered lines
File containing junk : /home/virgile/leaks/propre/tumblr.txt
Output will be sent to : out
Invalid lines will be sent to : err
Regex for /home/virgile/leaks/propre/tumblr.txt :
        Mandatory capturing groups : (?P<email>) and ( (?P<hash>) or (?P<plain>) )
        (Shortcuts : '$fast_email$','$sha1$','$md5$', '$posix_email$')
        $posix_email$ is RFC 5322 compliant (slow but accurate), $fast_email$ is 99.99\% accurate but 10x faster.
> $posix_email$:$sha1$:(?P<plain>.*)

Counting lines
        73361180 lines - 100.0%
Parsing file
        parsed : 11079680 (15.1%) - matching : 11079680 (100.0%) - creds : 11079680 (100.0%) - no/invalid mails : 0 (0.0%) - not utf8 : 0 (0.0%)
```

Quelques éléments techniques sur cet outil :

L'outil travaille sur place en mémoire, pour éviter de saturer la RAM de la machine qui s'en sert, même si le fichier à nettoyer est plus lourd que la quantité de mémoire allouable. Les entrées/sorties disque étant ce qu'il y a de plus lent dans l'exécution du programme, les lignes du leak initial sont lues par blocs de 4096 (configurable). Le programme pourrait être multi-threadé (option *nbThreads*), mais cela a peu d'intérêt pour les mêmes raisons (nombreuses entrées/sorties). Un affichage en temps réel est disponible, présentant des statistiques sur le travail en cours : nombre de lignes déjà analysées, nombre de lignes considérées comme valides (*matching*), nombre de lignes valides donnant lieu à un couple login/mot de passe, nombre de lignes sans mail valide (ou sans mail tout court) et nombre de lignes présentant des caractères avec lesquels nous ne pouvons travailler (non utf-8).
Performances : 350 000 lignes/seconde (matériel : Linux 4.13, Cpu i5 @ 2.50Ghz x4, le leak étant stocké sur un SSD).

Référencement des leaks et de leur contenu

Nous souhaitons maintenant aller plus loin que de simples fichiers texte, en intégrant toutes ces informations dans une base de données qui aura l'avantage de pouvoir accélérer les recherches. En soi, la recherche dans des fichiers est déjà possible, cela s'est notamment déjà vu avec l'archive Breach Compilation. Cette archive, trouvée sur un service caché fin 2017, a la particularité d'implémenter un index en forme d'arbre à deux niveaux sur les adresses mail. L'archive contient presque 2 000 fichiers servant à répartir les données. Si l'on recherche le mot de passe de l'utilisateur « toto@gmail.com », il est possible de rechercher directement dans le fichier « breachCompilation/data/t/o ». Dans notre cas, nous voulons rechercher des données à partir du nom de domaine du mail. Si l'on souhaite utiliser un index dessus, il faut séparer le mail en deux parties : le préfixe et le domaine (un mail sera sous la forme prefix@domain). Comme on souhaite avoir un outil rapide et efficace, le mieux à faire reste de structurer les données de la façon la plus simple possible.

POUR RENFORCER LA SÉCURITÉ DE VOTRE ENTREPRISE, GLISSEZ-VOUS DANS LA PEAU D'UN HACKER

INTRUSION

- Tests d'intrusion et sécurité offensive
- Tests d'intrusion avancés et développement d'exploits

Dates et plan disponibles
Renseignements et inscriptions
par téléphone
+33 (0) 141 409 704
ou par courriel à :
formations-cyber@deloitte.fr

Conception : SIMPUB - 06 50 88 11 01 - Crédit photo : Shutterstock - Creations

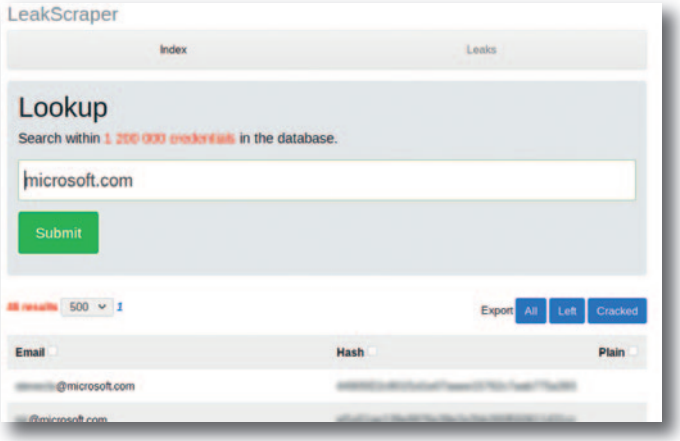
www2.deloitte.com

Deloitte.

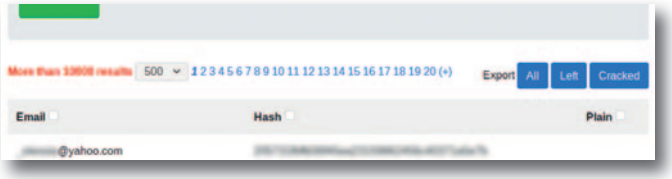
Le préfixe, partie gauche de l'email, ne nous servira pas, notre cas d'usage n'étant pas la recherche d'un utilisateur en particulier. Le domaine, en revanche, est l'information sur laquelle nous allons effectuer nos recherches. Nous aurons donc un index à créer. Le choix du type d'index est rapide : dans tous les SGBD nous avons globalement la possibilité de faire des index par Hashmaps ou des index en arbres (B-Tree). Les index en arbres ont l'intérêt de permettre des recherches efficaces par intervalles, ce dont nous n'avons pas besoin. De plus, la recherche d'une donnée parmi un tel index nécessite le parcours de l'arbre en question. Un index par hashmap, quant à lui, se contente de mapper directement un hash à un ensemble de valeurs. Un index par hashmap nous permettra donc d'accéder très rapidement à l'ensemble des credentials associés à un domaine. A côté de ces données, on stockera des informations sur les leaks intégrés à notre base, uniquement pour suivre son évolution et être capable de situer la quantité de données présente. Les leaks auront le format suivant : nom, nombre de credentials, nom du fichier initial.

LeakScraper

Nous avons ainsi développé un outil (nommé LeakScraper) permettant d'importer le plus vite possible des leaks standardisés dans une base mongo ou mysql. L'outil parcourt le leak standardisé et le transforme en CSV temporairement, puis importe le CSV dans l'un ou l'autre des SGBD. Ici encore, les erreurs pouvant survenir sont journalisées dans un fichier séparé pour garder une trace de toute donnée ayant posé un problème. Cette opération d'import pouvant être longue, un retour visuel de l'état d'avancement des opérations a été implémenté (cela a pris quelques heures pour importer les 1 400 000 000 de lignes présentes dans l'archive *BreachCompilation*).



Cet outil permet de rechercher efficacement (en temps et en mémoire) parmi nos quelques milliards d'enregistrements. Il permet au passage de télécharger rapidement les mots de passe qui nous intéressent (tous ou bien juste ceux que nous n'avons pas déjà cassés). Les résultats sont paginés, en étant affichés par défaut cinq cents par cinq cents. Pour plus de performances, le système de pagination a été paginé. Tant que nous avons moins de vingt pages d'identifiants à compter (10 000 résultats ou moins), tout se passe normalement, le nombre d'identifiants trouvé est affiché correctement, nous pouvons naviguer au sein des pages de résultats facilement. Au-delà de cette limite (le compteur de résultats indique alors « plus de 10 000 résultats »), nous pouvons naviguer parmi les vingt prochaines pages de résultats via un bouton « + ». Cela permet de ne jamais travailler qu'avec 10 000 résultats maximum à un instant T.



Ce choix (légère perte en fonctionnalité pour gain conséquent en performance) s'est fait assez simplement : nous n'allons (probablement) jamais obtenir plus de 10 000 résultats dans le cadre d'une utilisation nominale de l'outil. En effet, l'objectif étant de servir pour de l'OSINT en audit Red Team, il serait étonnant d'avoir autant de résultats liés à une entreprise donnée.

Pour conclure, tout le travail réalisé permet de partir sur de bonnes bases en matière de fouille dans un grand volume de données pouvant servir au cours d'un audit. Il est également important de rappeler que tout le travail a été fait sur un laptop, il n'est donc pas encore nécessaire de disposer d'une machine très puissante. Certains axes d'amélioration sont, en outre, à l'étude, visant à disposer :

- D'un outil capable de nettoyer la base de ses doublons, petit à petit, sans épuiser la mémoire de la machine ;
- D'un moyen permettant de mettre à jour des entrées dont les hashs auraient pu être cassés (ajouter le plain qui viendrait à manquer sur certaines entrées).

Tous les outils développés sont disponibles sur la page github d'ACCEIS : LeakScraper. ■■■

SÉCURISATION DE L'IOT INDUSTRIEL DÉPLOYÉ À GRANDE ÉCHELLE

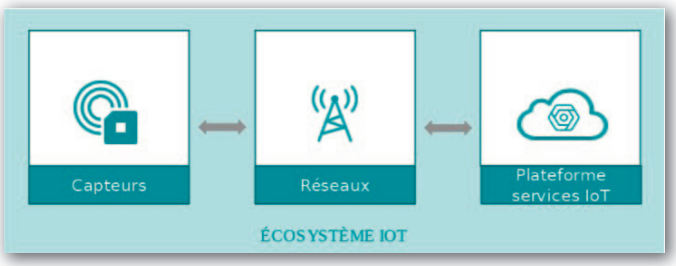
Par Quentin Heyler, expert en sécurité opérationnelle pour le cabinet ERIUM

L'Internet des Objets se développe massivement aujourd'hui dans les milieux industriels. Toutefois, l'écosystème IoT s'avère souvent peu propice à la sécurité, surtout dans des environnements aussi sensibles et spécifiques. Quelles sont les particularités de l'IoT industriel et les principaux risques inhérents à cet écosystème ? Et surtout comment renforcer la sécurisation de l'IoT industriel à grande échelle ?

Dans le milieu industriel, les objets IoT (Internet of Things) sont bien différents de ceux que nous pouvons croiser, voire utiliser au quotidien (smartphones, tablettes, montres connectées, appareils domotiques, enceintes Bluetooth, caméras de surveillance…). Il s'agit principalement de capteurs (objets captant une ou plusieurs données sur le terrain et chargés de la retransmettre à un dispositif de gestion centralisée ou plateforme) ou bien d'actionneurs (plus rarement observés toutefois), qui peuvent effectuer une action sur le terrain.

L'objet devient « connecté » lorsqu'il retransmet ses données ou bien reçoit des informations de la plateforme en transitant à un moment donné par l'Internet. Cette connexion s'effectue directement en TCP/IP ou bien en traversant un ou plusieurs réseaux 3G/4G, Wi-Fi, Bluetooth, Zigbee ou même des réseaux spécifiques à l'IoT LPWAN, comme Lora, Sigfox, etc. Comme dispositif de gestion centralisée, on peut trouver une ou plusieurs plateformes qui effectuent le lien avec l'utilisateur final.

Les 3 éléments suivants représentent l'écosystème IoT industriel :



Pour chacun de ces éléments d'infrastructure, on constate que le niveau de sécurité n'est pas homogène. Au niveau de l'objet, on considère que la sécurité est généralement faible. Elle est très variable pour les différents réseaux que peut traverser la donnée. En effet, beaucoup de réseaux IoT n'offrent pas les mêmes propriétés de sécurité (Intégrité, Confidentialité, protection Man-in-the-middle ou rejeu). Les plateformes présentent un niveau de sécurité généralement plus élevé, car il s'agit d'environnements plus facilement maîtrisables (Data Centers, serveurs). C'est bien sûr à vérifier au cas par cas.

Les différentes catégories d'objets

- Directement accessibles sur Internet (communiquant directement en TCP/IP) ou bien données/objets accessibles uniquement en passant par une plateforme tierce (d'un opérateur Lora ou Sigfox par exemple).
- Objet avec un OS « classique » (Linux…) adapté à l'embarqué ou juste un programme tournant sur un microcontrôleur.
- Administrable à distance ? Les accès d'administrations légitimes doivent être contrôlés, il peut s'agir juste de reparamétrage (changement d'un seuil de détection) ou bien d'administration complète en SSH.
- Un actionneur ou juste un capteur ? En général, lorsque l'objet agit sur l'environnement en actionnant un élément mécanique (ouverture d'une vanne, commande d'un ascenseur, etc.), les potentiels dysfonctionnements/compromissions sont bien plus problématiques…
- Objet agissant seul et relié avec le sol ou faisant partie d'une flotte d'objets qui communiquent entre eux ?
- Objet autonome énergétiquement ou non ? Dans le cas des objets qui sont uniquement sur batterie, les fonctionnalités sont limitées au juste nécessaire pour lui permettre de tenir sans alimentation pendant de longues durées, 5 ans ou plus… pas vraiment le cas d'un smartphone actuel !

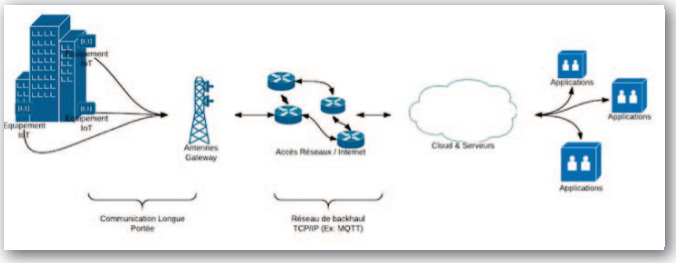
ACCOMPAGNER LES PROJETS POUR INTÉGRER LES BESOINS DE SÉCURITÉ

Avant même de chercher à analyser en profondeur la sécurité d'un objet, il est nécessaire de repositionner la donnée dans le contexte général du projet. Il existe, par exemple, une grande différence entre un objet qui récupère une donnée de type « température » ou « pression » utilisée dans un contexte non sensible, et une donnée d'un type similaire utilisée pour monitorer des cuves de produits toxiques au sein d'un processus métier sensible.
Les besoins de sécurité du projet, basés sur les critères fondamentaux de sécurité DICT (Disponibilité, Intégrité, Confidentialité et Traçabilité) et associés à une analyse de risques, permettent donc de définir le niveau auquel on devra placer les exigences et recommandations de sécurité pour le projet.

INTÉGRER LE CHIFFREMENT AU SEIN DES RÉSEAUX IOT

Afin d'apporter les deux propriétés de sécurité majeures aux communications que sont l'intégrité et la confidentialité, la meilleure option est d'utiliser le chiffrement pour protéger les données qui transitent sur le réseau.
Concernant les objets directement accessibles sur Internet et qui disposent d'un OS « classique », aucun problème ! On pourra choisir de se baser sur des technologies éprouvées comme le chiffrement TLS/SSL ou SSH.
En revanche, pour les autres objets qui utilisent des protocoles IoT, la tâche est plus ardue ! Il est possible de reposer uniquement sur les propriétés de sécurité offertes par les couches réseau, voire d'ajouter une couche de chiffrement supplémentaire, pour peu qu'on ait la main à la fois sur l'objet et sur la plateforme. Cette condition n'est malheureusement pas toujours vérifiée « dans la vraie vie », comme par exemple avec les capteurs vendus « sur étagère » qu'il est impossible de modifier.
Pour les réseaux LPWAN (Lora, Sigfox en premier), ils sont plutôt unidirectionnels (même si l'acquittement des trames est possible), ce qui rend impossible l'utilisation de protocole à base de « handshake » avant le transport de données chiffrées. L'objet émet, mais ne reçoit pas de réponses du serveur avec des données choisies. De plus, ils ne permettent de transporter qu'un très faible volume de données (à cause du Cycle Duty utilisé pour ne pas sur-occuper la fréquence utilisée). On notera, pour information, qu'on compte 140 messages de 96 bits pour Sigfox et environ 250 messages pour du Lora par jour et par objet connecté. Pour les messages reçus par l'objet, c'est une valeur bien plus faible : 4 messages reçus pour Sigfox et une dizaine pour Lora (ces limitations sont principalement dues aux opérateurs, comme Objenious ou Orange).
On constate donc aisément qu'il est impossible d'utiliser les mécanismes de chiffrements à base de renouvellement de clés privées de 4 096 bits sans y passer un certain temps !

Modèle standard d'architecture LPWAN :



Source : http://www.digitaldimension.solutions/blog/avis-d-experts/2016/02/lpwan-le-reseau-emergent-de-liot/

TECHNICAL REVIEW

Large scale deployment of industrial IoT security

By Quentin Heyler, Operational Security Expert for ERIUM

The Internet of Things is growing massively in industrial environments nowadays. Yet the IoT ecosystem often proves to be unsafe, all the more so in such sensitive and specialised environments. What are the characteristics of industrial IoT and the main risks typical of this ecosystem? And above all, how to set about strengthening industrial IoT security on a large scale?

Le secure element

Actuellement, c'est donc la cryptographie symétrique qui s'impose pour chiffrer les messages dans les communications entre les objets connectés et les plateformes, voire entre les objets. Le principe est d'utiliser la même clé pour chiffrer et déchiffrer le message. Dans la plupart des cas, la clé est écrite sur l'objet lors de sa fabrication, déposée à l'usine et stockée dans la mémoire physique de l'objet. C'est alors un microcontrôleur de l'objet qui effectue les opérations de chiffrement et de déchiffrement.
On note que le secret est stocké « en clair » dans la mémoire de l'objet, ce qui peut conduire à un risque de compromission de sa sécurité en cas d'accès physique à l'objet par un attaquant. La probabilité reste toutefois faible étant donné le fort niveau de connaissances techniques requis pour assurer la récupération de ce secret.
Afin de garantir un haut niveau de protection des secrets, on peut implémenter un tout petit composant : le « secure element » (imaginez un Cachou Lajaunie ;-)) qui contient les secrets et effectue les opérations cryptographiques. Il devient alors très compliqué, voire impossible pour un attaquant de récupérer un secure element et d'en extraire les informations recherchées. De plus, les spécifications techniques ne sont pas publiées.
Le prix d'un secure element est généralement de l'ordre de l'euro. En revanche, on observe que le véritable surcoût réside plutôt dans les phases de conceptions pour l'intégrer à l'objet.

Les algorithmes destinés à l'IoT et la standardisation

Il est temps de parler des algorithmes de chiffrement destinés aux IoT. En complément des contraintes réseaux, nos objets peuvent également hériter de performances limitées, tant au niveau de la puissance de calcul que de la consommation énergétique. Imaginons vouloir utiliser AES, pour chiffrer les messages de Sigfox (proposé sans chiffrement avant juillet 2017), la taille minimale des blocs étant de 128 bits, on ne peut pas envoyer le message en une seule fois… il est nécessaire de trouver des algorithmes qui permettent de répondre à ces nouvelles contraintes.
En fait, des initiatives existent, mais pour l'heure non standardisées. Le NIST a lancé en mars 2017 un processus de standardisation d'algorithmes spécifiquement destinés à l'IoT [1]. Cette initiative devrait nous permettre dans quelques années de pouvoir utiliser à grande échelle des implémentations de ces algorithmes. Et ce pourquoi pas dans des secure element !

Consommation énergétique du chiffrement

Pour les objets autonomes énergétiquement, un autre grand point d'attention sur le chiffrement est sa consommation énergétique. Le

les assises
de la sécurité et des systèmes d'information

ÉDITION LIMITÉE

10 › 13
octobre 2018
MONACO

@Les_Assises
#AssisesSI

2 800
PARTICIPANTS

5 200
RENDEZ-VOUS

170
ATELIERS
& CONFERENCES

COMEXPOSIUM

www.lesassisesdelasecurite.com

DG consultants

chiffrement entraîne bien une surconsommation de la batterie de l'objet. Mais contrairement à ce que l'on pourrait penser de prime abord, on constate que c'est plutôt l'émission du message en ondes hertziennes qui coûte à l'objet. Et ce, même avec des algorithmes non désignés pour l'IoT.

IMPLÉMENTER UNE GATEWAY

La gateway est un composant qui sert à étendre la couverture d'un réseau IoT. Dans certains cas (et on a souvent peu d'autres choix), il peut s'avérer nécessaire de déployer soi-même une gateway pour apporter de la connectivité. Par exemple, une gateway Lora pourra permettre l'écoute d'une partie de l'ensemble du trafic Lora émis aux alentours et le retransmettre en 3G/4G vers une plateforme distante.
Il est, dans tous les cas, déconseillé d'un point de vue sécurité que la gateway prenne en charge les fonctions de sécurité, telles que l'authentification des objets, le chiffrement… Il est préférable de réserver ce rôle à la plateforme. La gateway doit rester centrée sur la retransmission des messages, sinon cela impose la présence d'un référentiel d'objet (secret d'authentification ou chiffrement) qui peut éventuellement être récupéré si la sécurité de la gateway est compromise.
Si on souhaite néanmoins maintenir ces fonctions au niveau de la gateway et que le niveau de sécurité l'exige, il est alors nécessaire d'implémenter des mécanismes, tels que le chiffrement des secrets stockés par exemple sur un TPM, de durcir le hardware pour ne permettre le boot qu'à partir d'une source externe et de limiter l'accès aux interfaces d'administrations.

MAÎTRISER LES ACCÈS EN ADMINISTRATION ET LE DURCISSEMENT

Les accès d'administration permettent de prendre le contrôle de l'objet. Physiquement, cela peut se traduire par l'usage d'un port Jtag, USB, etc., qui peut permettre de réinjecter un nouveau firmware ou d'accéder à une interface de debug. Afin de renforcer le niveau de sécurité, on conseille que les accès d'administration physique ne soient accessibles qu'une fois le boîtier de l'objet ôté. Cela peut ralentir ou décourager un attaquant, mais il convient de noter que, sans sécurité supplémentaire, on peut considérer l'objet comme étant compromis en cas d'accès physique.
Pour un objet implanté à distance, on déconseille dans tous les cas que les interfaces d'administration soient exposées. Si elles le sont, la mise en place d'un processus de mise à jour sécurisé est alors incontournable pour se protéger des vulnérabilités encore inconnues.

Échange des secrets d'authentification et/ou de chiffrement

Les objets disposent de secrets (d'authentification ou de chiffrement) qui sont déposés dans l'objet à l'usine. Idéalement, cette action est effectuée depuis un poste dédié et les secrets ne sont partagés qu'avec les seuls correspondants ayant le besoin d'en connaître.
De plus, ils doivent être déposés sur la plateforme qui assure l'authentification, voire le chiffrement. L'échange de données sensibles avec des fournisseurs externes est souvent mal couvert par les outils des industriels. On constate qu'à l'usage, le mail chiffré, le mot de passe envoyé par SMS pour ouvrir le zip… sont mal suivis par les équipes, prennent trop de temps ou sont passés à la trappe.
Pérenniser une plateforme dédiée à l'échange des secrets, comme par exemple celle proposée par Shadline, est une bonne pratique et une impérieuse nécessité.

Le mot de passe par défaut

Il s'agit là de la faille du siècle pour l'IoT! Le malware Mirai et toute ses variantes encore en activité, qui ont infecté des centaines de milliers d'IoT, peuvent en témoigner.
Pour la petite histoire, en effectuant une pause durant la rédaction de cette chronique, je suis (encore) tombé sur un article croustillant qui montre un botnet IoT (Owari) compromettant de très nombreux objets en utilisant des mots de passe par défaut. Le plus « drôle », dans ce cas de figure, c'est qu'un chercheur en sécurité [2] a pu récupérer l'accès au serveur de contrôle du malware (le C&C), car celui-ci utilise le couple id/mdp : root/root pour protéger sa base de données… une sorte d'arroseur arrosé !

PLATEFORME IOT PRINCIPALE OU INTERMÉDIAIRE

Dans cet article, j'ai peu eu l'occasion de parler de la plateforme IoT qui centralise les données pour les mettre à disposition d'un utilisateur ou bien les retransmettre aux applications métier. La plateforme regroupe aussi l'administration des objets. C'est la partie émergée de l'iceberg. C'est elle qui doit implémenter certaines fonctions de sécurité indispensables comme authentifier les objets, sécuriser et chiffrer si possible le dernier réseau traversé (Internet).
Elle héberge également le référentiel d'objet. La gestion des droits met en jeu à la fois des capteurs qui produisent des données et des applications qui les consomment, voire même des applications ou objets qui envoient des messages (administration ou autre) directement aux objets. Une certaine traçabilité des modifications apportées par les humains est généralement souhaitable.
A cela doit s'ajouter la gestion d'au moins deux populations : simples utilisateurs et administrateurs.
Dans le milieu industriel, ces plateformes sont réutilisées par plusieurs directions, elles doivent donc posséder des propriétés de cloisonnement.

Les développeurs d'applications à base d'IoT préfèrent d'un point de vue opérationnel utiliser directement les « vraies » données de production sur les environnements de développements. C'est légitime, mais il n'y a en pratique jamais un objet qui peut être dédié à ces tests. Il s'agit d'objets utilisés en production. Par exemple, on ne peut pas simuler « une cuve de 300 litres » (il faut la cuve :-)).
On conseille de limiter à peu d'objets dans le temps l'utilisation des données de production sur les environnements hors production, tout en désactivant l'envoi de commandes à distance ou bien en monitorant spécifiquement ces actions lors d'expérimentations cadrées.
De leur côté, les acteurs majeurs du Cloud (IBM, Google, Amazon…) proposent des plateformes IoT, mais il s'agit plus de boîtes à outils qu'il est nécessaire de réutiliser à sa sauce, rien de magique. Néanmoins, les fonctionnalités sécurité que j'ai pu observer et tester étaient bien pensées et de qualité.

CONCLUSION

Le développement de l'IoT dans les milieux industriels a de beaux jours devant lui, même s'il profite d'un écosystème souvent peu propice à la sécurité, et que la culture « security by design » reste marginale. Pour se généraliser, la démarche sécurité devra prendre en compte les enjeux stratégiques des projets dès la phase de conception. ■■■

[1] https://csrc.nist.gov/publications/detail/nistir/8114/final
https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf
[2] https://blog.newskysecurity.com/hacker-fail-iot-botnet-command-and-control-server-accessible-via-default-credentials-2ea7cab36f72)

LE GRAND QUIZZ

TESTEZ VOS CONNAISSANCES SUR LES RED TEAM AVEC ARNAUD SOULLIÉ ET CHARLES IBRAHIM, WAVESTONE (PLUSIEURS RÉPONSES POSSIBLES).

Arnaud Soullié

1 Un exercice Red Team, c'est…

a. Un pentest, mais ça fait mieux de dire « Red Team »
b. Un scan de vulnérabilités et une phase d'exploitation
c. Un exercice visant à déterminer s'il est possible d'atteindre un objectif précis (accès à certains systèmes ou données)

2 L'équipe Red Team utilise généralement les moyens suivants :

a. Des attaques logiques (tests d'intrusion)
b. Des attaques logiques et physiques
c. Des attaques logiques, physiques et d'ingénierie sociale

3 Un rapport Red Team, c'est…

a. Pas de rapport, on est là pour tout défoncer
b. Des preuves de l'atteinte de l'objectif, et une explication détaillée de la méthodologie et des actions menées
c. Un plan d'action très précis pour améliorer globalement son niveau de sécurité

4 Une équipe Red Team, c'est…

a. Une équipe avec un maillot rouge présente à la coupe du monde
b. Des pentesteurs en cagoule devant leur PC
c. Une équipe pluridisciplinaire, avec des compétences techniques, mais aussi des analystes avec des compétences métiers

5 Une Red Team suit une méthode normée :

a. ISO 27042
b. Aucune, c'est forcément spécifique
c. PASSI v2.3

6 La démarche d'attaque lors d'un exercice Red Team s'appuie sur…

a. Toute technique pouvant mener à l'atteinte de l'objectif fixé initialement
b. Un test d'intrusion Web standard
c. Une démarche cadrée : revue de configuration, entretien et test d'intrusion sur un périmètre identifié

DE SENSIBILISATION

ÉTÉ 2018

Par Arnaud Soullié, Manager, et Charles Ibrahim, Consultant - Wavestone

Charles Ibrahim

7 Je peux commander un exercice Red Team si…

a. Je ne connais pas mon niveau de sécurité et j'ai besoin de premières réponses
b. J'ai besoin d'un pentest, mais je veux des pentesters plus techniques
c. Je pense maîtriser ma sécurité, je réalise déjà des tests d'intrusion classiques et ils ne sont pas catastrophiques

8 Les outils pour un exercice Red Team, c'est…

a. Nessus & Metasploit
b. Des 0-days et des outils développés spécialement pour l'exercice
c. L'outillage qui fonctionne, l'équipe s'adapte à la situation et à l'objectif

9 Le périmètre d'un audit Red Team, c'est…

a. Un périmètre large, réaliste vis-à-vis de ce que pourrait faire un attaquant
b. Une application bien précise
c. HACK THE PLANET!

10 Une Red Team peut mobiliser :

a. Un pentester
b. Un reverser
c. Un chasseur de tête

Retrouvez les solutions page 52

© AridOcean

Certification HDS : la pilule risque d'être difficile à avaler pour certains opérateurs

Par Marc Jacob et Emmanuelle Lamandé

L'agrément d'hébergeur de données de santé a laissé place depuis le 28 février 2018 à une certification. Cette refonte en profondeur suscite de nombreux débats auprès des principaux intéressés que sont les opérateurs de Data Centers et les fournisseurs de services. Si pour les grands offreurs, ce n'est qu'un nouveau processus de plus à mettre en place, pour les opérateurs de plus petite taille, la pilule risque d'être plus difficile à avaler… Alors va-t-on une fois de plus dans ce pays favoriser les grands groupes au détriment des PME ? Quid des établissements de santé qui pourraient voir disparaître certains de leur fournisseurs…

Fabrice Coquio, Interxion France

L'ASIP a lancé le 28 février 2018 la certification HDS visant à remplacer l'agrément d'hébergeur de données de santé. Cette refonte était nécessaire pour donner plus de transparence à l'attribution des précédents agréments. Toutefois, les contraintes inhérentes à la certification risquent de laisser sur la touche un certain nombre d'opérateurs et de fournisseurs, notamment ceux de petite taille. En effet, ces derniers avaient déjà dû réaliser des efforts conséquents pour obtenir l'agrément. Ils vont devoir aujourd'hui remettre la main à la poche s'ils souhaitent répondre aux exigences de la certification, et ce dans des délais relativement courts au vu de la tâche à accomplir pour certains. C'est sans doute pour cela que bon nombre d'opérateurs de Data Centers qui ont un agrément ont aujourd'hui refusé de répondre à nos questions, du fait, selon leurs dires, de la charge supplémentaire demandée pour le passage à la certification. D'ailleurs, François Kaag, Président de l'AFHADS, avait expliqué dans le N°42 de Global Security Mag que « ce décret vise à la banalisation de l'Hébergement de Données de Santé. La certification reste favorable aux grands hébergeurs généralistes et aux éditeurs globaux. En revanche, elle est défavorable aux autres acteurs qui perdent un appui compétent et un contrepoids aux éditeurs globaux ». Effectivement, pour les grands opérateurs, comme SFR ou Interxion, ayant obtenu l'agrément depuis de nombreuses années déjà, cette évolution ne semble pas poser beaucoup de problèmes. Ainsi, pour Pascal Rehm, Responsable hébergement chez SFR Business, qui a obtenu un agrément en tant qu'infogéreur, ce passage ne devrait pas s'avérer problématique. Il sera d'ailleurs une priorité, d'autant que son entreprise aspire à être certifiée en tant qu'infogéreur et hébergeur d'infrastructure physique.

Dans le passé, l'obtention de l'agrément était relativement longue et parfois obscure. Ainsi, Fabrice Coquio, Président d'Interxion France, se rappelle qu'auparavant l'agrément HDS ne faisait pas de différence entre hébergeur d'infrastructure physique et hébergeur infogéreur. « Nous avions même pris un avocat, afin de pouvoir séparer la partie opérateur d'infrastructure physique de celle d'hébergeur infogéreur. Il nous a fallu environ un an pour obtenir cet agrément, qui nous a été délivré en 2014. Nous étions les seuls au début à l'avoir obtenu. L'évolution vers une certification va permettre de clarifier le « qui fait quoi ». En effet, elle définit deux types de certificats : d'un côté, celui des hébergeurs d'infrastructures physiques et de l'autre celui des hébergeurs infogéreurs. » De son côté, Nicolas Pitance, Président de DCforDATA, avait déposé son dossier en juin 2016, mais n'a obtenu l'agrément que le 15 mars 2018. Cette si longue durée est, selon lui, liée au fait d'avoir choisi un certificateur inconnu de l'ASIP… SynAApS, pour sa part, comme l'explique Rémi Grivel, son Directeur Général, a obtenu en premier lieu la certification ISO 27001:2013 en novembre 2014, délivrée par Bureau Veritas, pour l'intégralité de ses infrastructures et services PaaS-IaaS-Housing. Puis, en août 2015, l'entreprise a également reçu l'agrément d'Hébergeur de Données de Santé (HADS) par le Ministère français de la Santé, en accord avec l'ASIP Santé et la CNIL. Avec cet agrément HADS, SynAApS a ouvert ses Data Centers aux professionnels médicaux et à leurs prestataires techniques pour l'hébergement sécurisé de leurs données de santé. « Nous avons initié ces deux démarches en même temps, celles-ci présentant certaines similitudes. En effet, les exigences inhérentes à l'agrément HADS représentent environ 60% des obligations ISO 27001. » Ainsi, selon Rémi Grivel, il est clair que « dans la continuité logique de notre agrément HADS et certification ISO 27001 :2013, nous allons bien entendu effectuer une demande de certification auprès de l'ASIP Santé, pour l'ensemble des briques de ces deux catégories. Notre démarche étant déjà initiée et nos process en conformité, le pas vers la certification HDS ne sera globalement qu'une formalité. Toutefois, il n'en sera pas de même pour tous les acteurs. En effet, la certification HDS impose entre autres aux postulants d'être certifiés ISO 27001, ce qui n'était pas le cas auparavant avec l'agrément. La démarche de mise en conformité, en vue de l'obtention de la certification HDS, sera donc beaucoup plus importante pour les acteurs agréés HADS n'étant pas certifiés ISO 27001 ».

Le passage à la certification sera pour certains opérateurs bénéfique, dans la mesure où celle-ci va permettre de clarifier certains points. Camille Cacheux, Directeur Général de Coreye Healthcare du Groupe Pictime,

Camille Cacheux, Coreye Healthcare

qui va faire une demande en priorité pour être certifié infogéreur et, dans un second temps, hébergeur d'infrastructure physique, estime que déconnecter la partie infogéreur et hébergeur d'infrastructure physique est globalement cohérent. « Nous travaillons en mode multi-cloud. En fait, notre vision est de piloter les applications pour les établissements de santé en multi-cloud. Ainsi, cela nous permet d'accompagner les établissements de santé vers le cloud en intégrant la sécurité. Nous avons donc une offre de services pour la partie infogérance et SOC externalisé de santé. Nous sommes déjà certifiés Azur, AWS et VMware. » De plus, il considère que « même si a priori il n'y a plus de co-responsabilité pour les infogéreurs, dans tous les cas, au titre du RGPD, les sous-traitants sont co-responsables de traitement et ont devoir de conseil à minima. Effectivement, pour l'hébergeur pur, il n'y aura pas de co-responsabilité. »

Fabrice Coquio, pour sa part, regrette que la certification soit uniquement limitée aux frontières nationales, et que le législateur ne l'ait pas étendue au niveau européen. « Par exemple, pour les laboratoires pharmaceutiques qui ont des besoins de reconnaissance à l'international, cette certification ne répond pas à leur demande. Ce nouveau cadre est extrêmement restrictif. Toutefois, avec cette certification, la France reste en avance sur les autres pays européens. Est-ce que ce référentiel s'imposera à terme en Europe ? Ce serait une bonne chose, mais rien n'est encore joué. D'ici la fin 2018, ce n'est pas sûr que ce problème soit résolu, d'autant que les premières certifications seront à peine délivrées. Sans compter qu'un vide va néanmoins demeurer entre aujourd'hui, où il n'y a plus d'agrément, et le début de la certification. Les choses ne se clarifieront pas avant la fin de l'année 2018. »

LA CERTIFICATION ASIP, UN CENTRE DE COÛT ?

En termes de coût, la nouvelle certification risque d'être relativement onéreuse. Malgré les nouveaux budgets demandés en vue d'obtenir l'agrément, tous les opérateurs interrogés vont prétendre à la certification dans leur domaine. D'autant que, pour certains, il en va de la survie d'au moins une partie de leur entreprise. Fabrice Coquio considère que « pour un acteur qui s'appuie déjà sur la norme ISO 27001, le passage à la certification ne requiert pas un travail fondamental. En effet, nos infrastructures étaient largement compatibles avec l'agrément, et la norme ISO, et le seront désormais avec la certification. Les obligations relatives à la certification HDS ne présentent pas un problème pour nous. Au contraire, elles vont même quelque peu écrémer le marché en contrôlant, et donc en validant, les éléments déclaratifs sur la partie essentielle : l'infrastructure physique. Bien sûr, cette démarche (soumission, suivi…) nécessite du temps. Même avec toutes nos certifications (ARJEL, PCI-DSS, ISO 50001…), l'étendue de nos activités nous oblige depuis des années à avoir ce niveau d'exigences avec nos différentes certifications. Toutefois, la certification HDS ne va pas engendrer d'investissements dans nos infrastructures ou nos process. Nous avons estimé le coût du passage de l'agrément à la certification à une vingtaine de jours/homme. Nous pensons que l'obtention de la certification nécessitera moins de charge de travail pour tout acteur déjà certifié ISO 27001. Lorsque nous avions obtenu l'agrément, nous n'avions pas modifié notre grille tarifaire.

DATA CENTER

"HDS" certification: the pill may be difficult to swallow for some operators

By Marc Jacob and Emmanuelle Lamandé

From the 28 February 2018 approval of health data hosting (HDS) has been subject to a certification process. This major overhaul sparked a lot of debate among key stakeholders, notably data center operators and service providers. While for large suppliers this may well be just another process to set up, for smaller operators the pill may be more difficult to swallow ... So once again are we, in this country, going to accommodate large groups at the expense of SMEs? What about health facilities that could see some of their suppliers disappear ...

Nicolas Pitance, DCforDATA

Il en sera de même pour la certification. Ce marché touche aussi bien nos Data Centers de Paris que ceux de Marseille. Il concerne donc des éditeurs de tailles diverses, répartis tant à Paris qu'en régions. » Nicolas Pitance évalue, quant à lui, ce coût à 50 000 euros, « mais cette fois-ci je prendrai un organisme certifié », a-t-il promis. De son côté, Rémi Grivel fait un inventaire des différentes sources de coûts qui sont à prévoir dans une démarche de certification : « le cabinet qui vous accompagne dans cette mise en conformité, le bureau qui va venir vous auditer, sans compter les ressources nécessaires en interne. Pendant les deux années de préparation nécessaires à la certification ISO 27001 et à l'agrément HADS, une personne, à savoir notre RSSI, a travaillé exclusivement chez SynAApS à cette mise en conformité. Depuis, nous avons également recruté un DPO/juriste, en charge de cette partie certification et mise en conformité RGPD. Cet investissement nous a permis de nous inscrire à présent dans une démarche vertueuse, intégrant la conformité et la sécurité par essence dans toutes les phases de développement du groupe et de ses services. Le passage de l'agrément à la certification devrait d'ailleurs en être facilité. Nous estimons ce coût à 15/20 000 euros environ. Cependant, il ne faut pas perdre de vue qu'une certification ne se fait pas uniquement à un instant T. Elle s'inscrit dans une démarche d'amélioration continue et d'audits réguliers de conformité. Pour être efficiente, il est essentiel que la direction et l'ensemble des équipes soient impliquées dans cette démarche. La conformité doit reposer sur une véritable méthode de travail vertueuse, et non se faire sous la contrainte. C'est l'ensemble de ces éléments qui permettra de renforcer la structure, mais aussi la sécurisation des hommes et des process ». Quant à Camille Cacheux, il

Espace Saint-Martin - Paris

DATA CENTER

Le 14 novembre 2018

LE DATA CENTER DANS TOUS SES ÉTATS

Crédit image : © Sweet Art

Global Security Mag

DE LA THÉORIE À LA PRATIQUE

COLLOQUE

De la théorie à la pratique

en partenariat avec : FRANCE DATACENTER - EUDCA - AN2V - Forum ATENA - CLUSIF

SPONSORS

SAPHIR

DATA4 DATA CENTERS AT SCALE

VERTIV

BRONZE

R&M

STEPHYA DataCenter Global Services

ASSOCIÉ

ebrc TRUSTED DATACENTRE, CLOUD & MANAGED SERVICES

Tarif d'inscription au colloque :

Journée complète inclus les pauses café, le repas du midi et le cocktail de clôture : 120€ HT (TVA 20%)

Déclaration d'activité enregistrée sous le numéro 11 92 17185 92 auprès du préfet de région Ile-de-France

Pour plus d'informations : http://www.globalsecuritymag.fr/De-la-theorie-a-la-pratique/ ■ **Attention, le nombre de places est limité.**

Le planning de la journée sera publié prochainement sur le site : http://www.globalsecuritymag.fr/De-la-theorie-a-la-pratique/

Contact : Marc Jacob Brami - Tél. : 01 40 92 05 55 - marc.jacob@globalsecuritymag.com

estime que « ce coût sera sans doute important, même si nous sommes déjà certifiés ISO 27001. Par contre, il est demandé d'accompagner les établissements de santé dans l'infogérance et le pilotage d'application. Tout dépendra des cabinets de certifications, du niveau de départ et des plans de progrès. Si la barre est trop haute, il risque d'y avoir des hébergeurs qui ne suivront pas cette démarche. J'estime ce coût entre 120 et 180 jours/hommes, sans compter celui de l'organisme de certification. Dans le passé, nous avions un audit tous les 3 ans. Si la barre est plus élevée, cela risque d'augmenter la facture et de rogner sur nos marges, dans la mesure où les établissements de santé n'ont pas des budgets extensibles. »

CERTIFICATION ASIP, UNE BONNE AFFAIRE EN TERMES DE CA ?

La certification ASIP, si elle est source de coût, peut-elle être une bonne affaire en termes de recette ? En fait, tout dépend de la taille et de la stratégie de l'opérateur. Selon Camille Cacheux, l'obtention de la certification sera une nécessité, d'autant que pour sa filiale elle représente 100% du CA, mais aussi 15% du CA de son groupe. De même pour Nicolas Pitance, qui a mis 2 ans à obtenir l'agrément et pense obtenir 30% de son CA grâce à ses certifications ISO 27001 et/ou ASIP qui sont de plus en plus exigées par les clients : « nous avons déjà la certification ISO 27001 depuis septembre 2015. Nous comptons depuis longtemps parmi nos clients des acteurs de la santé. Nous pourrons de ce fait adresser des infogéreurs et de grands acteurs de la santé qui sont déjà chez nous. Nous avons donc des commandes depuis le 15 mars 2018, mais elles n'ont pas encore généré de CA. » Selon Fabrice Coquio, l'obtention de la certification fait partie d'une stratégie plus globale. « Le groupe se doit d'être présent dans tous les secteurs. Quatre ans après l'obtention de cet agrément, nous avons gagné plusieurs dizaines de contrats, mais je ne parle pas ici d'établissements de santé, comme des hôpitaux. En effet, la plupart de nos clients sont des éditeurs et des ESN qui proposent des services infogérés. Ils ont donc besoin de s'appuyer sur une infrastructure qui leur manquait. C'est un marché qui a un certain intérêt, mais qui reste un segment assez faible aujourd'hui. » Quant à Pascal Rehm, il évalue les recettes de ce domaine d'activité à 10% de son CA. Rémi Grivel considère que « l'hébergement de données de santé représente aujourd'hui environ 15% de notre chiffre d'affaires. A noter toutefois que nos clients opérant dans d'autres domaines que celui de la santé bénéficient aussi de la même qualité d'hébergement et du même niveau de sécurité. »

QUID EN TERMES D'IMAGE ?

Rémi Grivel, SynAApS

Si Rémi Grivel estime que « cette certification n'aura pas d'impact sur notre business à proprement parler, dans la mesure où elle s'inscrit uniquement dans la continuité de notre démarche et de nos actions initiées il y a plusieurs années déjà. » Pour tous nos autres experts, l'obtention de la certification aura sans nul doute des implications positives au moins en termes d'image. Pascal Rehm explique que « sur différents appels d'offre, on a cette obligation. Cette certification va devenir un prérequis sur beaucoup d'appels d'offres et va donc avoir des répercussions sur les revenus dans cette activité ». Effectivement, reprend Nicolas Pitance, « la certification va créer une véritable barrière à l'entrée, mais elle permettra de distinguer les Data Centers. Elle est un facteur différenciant, mais aussi d'excellence opérationnelle en France. Cela nous permet de professionnaliser le métier et nous oblige à avoir un véritable devoir de conseil ». En effet, rappelle Camille Cacheux, « dans le passé, l'agrément sous la forme du « déclaratif » ouvrait le marché à des entreprises, qui pouvaient tirer les prix vers le bas, en rognant sur les services ou par manque de professionnalisme. La certification va donc un peu écrémer le marché en faveur de véritables professionnels du domaine. Par contre, si la barre est trop peu élevée ou trop basse, on pourrait retomber dans les mêmes travers qu'avec l'agrément. » Enfin, Fabrice Coquio considère que la certification va « permettre de montrer que nous savons accompagner nos clients dans tous les segments de marché, comme nous savons le faire dans d'autres domaines, comme l'assurance, le jeu… Au niveau du grand public, cela a aussi un impact. En termes de CA, le secteur de la santé est profitable, mais reste mineur en France. Nous pensons qu'il y aura également des retombées dans le domaine de l'assurance, dans la mesure où ce dernier propose aussi aujourd'hui des prestations de santé. Il faut être positif sur cette certification, qui démontre un réel effort pour structurer le marché de la santé. Toutefois, il reste encore l'enjeu européen qu'il est urgent de résoudre, par exemple via la reconnaissance de la certification française au niveau de l'Europe. La certification est un gage de sérieux. De plus, la séparation entre les hébergeurs d'infrastructure physique et les hébergeurs infogéreurs était nécessaire. Même s'il reste encore des actions à mener pour accélérer le processus de certification, cette dernière va donner les moyens de sécuriser les données, mais aussi de baisser les coûts de fonctionnement des organismes de santé via, entre autres, la mutualisation des infrastructures. » ■■■

© AridOcean

L'hébergement neutre en colocation et la responsabilité relative à la protection des données

Par Anthony Coquer, Département Sécurité & Organisation, Lexing Alain Bensoussan Avocats

Les opérateurs de Data Centers neutres se posent aujourd'hui la question de leur responsabilité face au RGPD. En effet, dans la mesure où ils ne font que louer des espaces en fournissant l'électricité, les télécoms et la climatisation, cette interrogation semble légitime…

En 2017, selon l'enquête sur les technologies de l'information et de la communication et le commerce électronique de l'INSEE [1], 67% des entreprises françaises sont équipées d'un site Web en propre ou en partagé. Ces sites permettent, pour la majorité, de proposer des biens ou des services, ainsi que des listes de prix. Ils peuvent également offrir la possibilité de commander et réserver des produits ou services.

De nombreuses entreprises décident d'externaliser l'hébergement de leurs sites pour bénéficier de la mise à disposition de ressources appropriées (espace de stockage ou bande passante par exemple), de la sécurisation de la solution hébergée, ainsi que les conseils et services de support associés.

Pour héberger leurs vitrines en ligne, les entreprises disposent de plusieurs solutions en sous-traitance adaptées à leurs usages et à leurs moyens :

- **L'hébergement dédié** qui permet au client de disposer de son propre serveur qu'il peut en général administrer comme il le souhaite. Le prestataire reste cependant propriétaire du serveur. Cette solution coûteuse nécessite également de disposer des compétences spécifiques pour administrer le serveur.
- **Les hébergements dédiés managés** permettent l'infogérance du serveur. Le client dispose toujours de son propre serveur, mais le prestataire d'hébergement est en charge de la gestion du système.
- **L'hébergement partagé (ou mutualisé)** est la forme la plus courante d'hébergement. Afin de réduire les coûts, le même serveur est ainsi partagé par plusieurs clients différents. Le client mutualisé ne dispose pas des moyens pour administrer le serveur et la configuration est proposée par le prestataire.
- **L'hébergement virtuel dédié** est mis en œuvre via un hyperviseur. Le client accède à une machine virtuelle qui utilise une partie des ressources d'un serveur physique grâce aux techniques de virtualisation. La solution associe la souplesse des solutions dédiées tout en cloisonnant logiquement les espaces des clients.
- **L'hébergement neutre en colocation** (housing en anglais) diffère des autres formes d'hébergement (hosting en anglais). Le prestataire fournit l'infrastructure pour accueillir les serveurs des clients, l'alimentation électrique et la bande passante, ainsi qu'un certain nombre de services et de garanties comme l'accès sécurisé.

Le règlement (UE) 2016/679 du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), impose ainsi au responsable du traitement de mettre en œuvre les mesures techniques et organisationnelles appropriées, afin de garantir un niveau de sécurité adapté au risque.
A défaut de respecter les obligations du RGPD, le responsable du traitement peut se voir infliger des amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une en-

treprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Le sous-traitant, au sens du RGPD, est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.
Par traitement, il faut considérer toute collecte, enregistrement, organisation, structuration, conservation, adaptation ou modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, limitation, effacement ou destruction des données à caractère personnel.

Le traitement des données à caractère personnel peut impacter la vie privée des personnes concernées. Parmi les risques relatifs à la vie privée, il est nécessaire de considérer l'accès illégitime aux données (défaut de confidentialité), la modification non désirée des données (défaut d'intégrité), ainsi que la disparition des données (défaut de disponibilité). Dans ce dernier cas, nous pouvons imaginer, par exemple, que la non détection d'une interaction médicamenteuse du fait de l'impossibilité d'accéder au dossier électronique du patient puisse impacter l'intégrité physique de la personne concernée.

RGPD : LES OPÉRATEURS DE DATA CENTERS NEUTRES ONT UNE RESPONSABILITÉ LIMITÉE

Les obligations des prestataires fournissant une solution d'hébergement neutre en colocation sont limitées. En effet, le prestataire ne peut pas être qualifié de sous-traitant dès lors qu'il n'accède pas aux données à caractère personnel. De même, le prestataire qui ne détermine pas les finalités et les moyens du traitement n'est pas considéré comme responsable conjoint du traitement.
Il faut cependant considérer les impacts sur la vie privée liés à l'indisponibilité de l'hébergement ou de la bande passante. A l'image de la panne d'OVH, numéro un européen de l'hébergement de sites Internet qui, en novembre 2017 et suite à un défaut d'alimentation électrique, rendait indisponibles tous les sites et services hébergés.

Les contrats qui lient les prestataires d'hébergement neutre en colocation et le responsable du traitement doivent donc préciser les mesures techniques et organisationnelles appropriées qui doivent être mises en œuvre pour assurer notamment la disponibilité des données. Ainsi, en cas d'inexécution du contrat, la responsabilité contractuelle du prestataire pourra être engagée. Le responsable du traitement demeure cependant responsable des manquements et peut être sanctionné par la Commission Nationale de l'Informatique et des Libertés (CNIL). ■■■

[1] https://www.insee.fr/fr/statistiques/3535964?sommaire=3535969&q=site+web

DATA CENTER

Carrier neutral colocation housing and responsibility for data protection

By Anthony Coquer, Security & Organization Department, Lexing Alain Bensoussan Avocats

Operators of neutral Data Centers are now raising the question of their responsibility with regard to the GDPR. This is indeed a legitimate question considering they simply offer rented spaces with provision of associated services: electricity, telecoms and air conditioning ...

BULLETIN D'ABONNEMENT

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE
N° 43

❒ Je souscris un abonnement à Global Security Mag pour une durée d'un an au prix de 60€ TTC (TVA 20%), 75€ hors France Métropolitaine et étranger. Je recevrai les 4 prochains numéros.
❒ ou je commande le numéro : ..... au prix unitaire de 24€ TTC (TVA 20%)

❒ Abonnement annuel au format PDF du magazine 33€ TTC (TVA 20%) ❒ ou je commande le numéro : ..... au format PDF 12€ TTC (TVA 20%)

❒ Abonnement couplé pour une durée d'un an, magazine papier et PDF au prix de 75€ TTC (TVA 20%)

❒ Je souhaite être abonné gratuitement à la News Letters hebdomadaire voici mon adresse mail : .....

❒ Je suis RSSI, DSI, Risk Manager, Administrateurs Réseaux – Télécoms, Sécurité et je souhaite être abonné au Service Gold de Global Security Mag. Je suis informé que ce service comprend des invitations VIP sur des événements de sécurité, des remises spéciales à des séminaires de sécurité, des invitations aux événements de sécurité organisés par Global Security Mag. En revanche Global Security Mag s'engage à ne jamais louer à titre gracieux ou marchand mes coordonnées personnelles ou professionnelles. Pour bénéficier de ces avantages, je joins ma carte de visite professionnelle (agrafer ici)

et mon adresse mail : ..... Je recevrai par mail une fois par semaine des informations ciblées

Nom ..... Prénom ..... Société .....

Adresse .....

Tél. ..... Fax. ..... E-mail .....

Règlement par chèque n° ..... Tiré sur banque à l'ordre de SIMP

A réception de votre règlement une facture acquittée vous sera adressée par retour.
Aucun abonnement ne sera accepté sans un règlement préalable de la totalité de son montant.

Date, Signature et cachet de l'entreprise

A retourner à :
SIMP
17, av. Marcelin Berthelot
92320 Châtillon
Tél. : 01 40 92 05 55
E-mail : ipsimp@free.fr
marc.jacob@globalsecuritymag.com

© Adrian Grosu

En application de l'article 27 de la loi du 6 janvier 1978, les informations ci-dessus sont indispensables au traitement de votre commande et sont communiquées aux destinataires la traitant. Elles peuvent donner lieu à l'exercice du droit d'accès et de rectification auprès de S.I.M. Publicité. Vous pouvez vous opposer à ce que vos noms et adresses soient cédés ultérieurement.

SOLUTIONS QUIZZ DE SENSIBILISATION

Arnaud Soullié et Charles Ibrahim, Wavestone

1. c
2. c
3. b
4. c
5. b
6. a
7. c
8. c
9. a
10. a - b - c

HS2
Hervé Schauer Sécurité

Formation cybersécurité technique

PROGRAMME

Introduction à la cybersécurité

ESSCYBER :
Essentiels techniques de la cybersécurité
SECUCYBER :
Fondamentaux techniques de la cybersécurité

Sécurité des réseaux et des infrastructures

SECUINDUS :
Cybersécurité des systèmes industriels
SECURSF :
Sécurité des réseaux sans fil
DNSSEC :
DNSSEC
SECUPKI :
Infrastructures de clés publiques
SECUPKIWIN :
Infrastructure de clés publiques Windows

Sécurité défensive et Réponse aux incidents

SECUWEB :
Sécurité des serveurs et des applications Web
SECUWIN :
Sécurisation des infrastructures Windows
SECULIN :
Sécurité Linux
SECUARCH :
Conception d'architectures sécurisées
SECUBLUE :
Surveillance, détection et réponse aux incidents de sécurité

Inforensique

FORENSIC1 :
Analyse inforensique Windows
FORENSIC2 :
Analyse inforensique avancée
REVERSE1 :
Rétroingénierie de logiciels malfaisants

Sécurité offensive

PENTEST1 :
Test d'intrusion
PENTEST2 :
Test d'intrusion et développement d'exploits

iStock
idcomm.fr

+33 644 014 072

www.hs2.fr

formations@hs2.fr

KASPERSKY lab

Détection des APT que les solutions de sécurité traditionnelles ne voient pas.

La plateforme Kaspersky Anti Targeted Attack allie algorithmes de machine learning avancés, Threat Intelligence et infrastructure évolutive.

- Une architecture de sondes multiniveaux pour une visibilité à 360°
- Une sandbox performante pour identifier les nouvelles menaces et les signes d'intrusion
- Des moteurs d'analyse puissants pour des diagnostics rapides et moins de faux positifs
- Des sources fiables de veille stratégique pour alimenter votre SOC
- Une corrélation permanente des évènements pour déceler les signaux faibles

Détectez si votre entreprise est victime d'une attaque ciblée et réagissez !

Kaspersky Anti Targeted Attack Platform

LA PLUS TESTÉE*
LA PLUS RÉCOMPENSÉE*
PROTECTION KASPERSKY LAB
*www.kaspersky.fr/top3

20 ANS DE RECHERCHE EN CYBERSÉCURITÉ

© 2017 AO Kaspersky Lab. Tous droits réservés.