Cybersécurité

Top 10 des incidents

economie
SPF Economie, P.M.E., Classes moyennes et Energie

.be

economie
SPF Economie, P.M.E., Classes moyennes et Energie

Cette publication constitue un extrait du manuel
« Cybersécurité - Votre entreprise est-elle prête ? ».

Service public fédéral Economie, P.M.E., Classes moyennes et Energie
Rue du Progrès 50
1210 Bruxelles
N° d'entreprise : 0314.595.348
https://economie.fgov.be

tél. 0800 120 33 (gratuit)

facebook.com/SPFEco

@SPFEconomie

youtube.com/user/SPFEconomie

linkedin.com/company/fod-economie (page bilingue)

Editeur responsable : Jean-Marc Delporte
Président du Comité de direction
Rue du Progrès 50
1210 Bruxelles

Version internet

209-18

© angelldeco - Fotolia.com

Chaque année, les différents Computer Emergency Response Team (CERT) des Etats membres publient les statistiques relatives aux incidents constatés sur leur territoire.

L'ENISA (European Network and Information Security Agency) compile ensuite les informations et publie un rapport annuel présentant les menaces constatées en Europe. Certaines grandes catégories (malwares) peuvent recouvrir d'autres types d'incidents (ransomwares, phishing...).

Voici le top 10 des incidents les plus constatés en Europe en 2017 ainsi que quelques bons réflexes à acquérir en fonction du type d'incident.

1. Malware

Les malwares les plus fréquents en 2017 ont été les ransomwares et les vols d'informations mais il en existe bien d'autres : chevaux de Troie (Trojans), PUPs (Potentially Unwanted Programs), droppers, Command & Control (C&C), key loggers, backdoors....

Les bons réflexes sont notamment :

- ne pas se reposer sur un anti-malware unique (privilégier multi-scanner/multi-canaux) ;
- prévoir une détection sur les différents canaux utilisés (intranet, internet, plateformes, PC, GSM...) ;
- prévoir une politique de sécurité et un incident management plan avec un point concernant les malwares ;

© momius - Fotolia.com

- prévoir des outils d'analyse sur les malwares et se tenir informés des dernières tendances ;
- réaliser des tests réguliers et mettre en place un monitoring.

2. Web-based attacks

Les attaques « Web based attacks » portent en général sur les browsers (Google, Mozilla, Safari...) et sur leurs extensions ainsi que sur les systèmes de gestion des contenus (Content management Systems ou CMS comme WordPress, Drupal, Joomla...).

Les bons réflexes consistent notamment :

- à mettre à jour (patcher) régulièrement afin d'appliquer les correctifs de sécurité ;
- à prévoir une protection contre les softwares connus pour être vulnérables et non patchés ;
- à préférer une identification à plusieurs facteurs (politique des mots de passe...) ;
- à modifier le préfixe par défaut de la base de données (par exemple wp_ pour WordPress) ;
- à prévoir un point de restauration régulier ;
- à détecter et filtrer les browsers plug-ins (ne provenant pas de sites officiels).

3. Web application attacks

Les attaques « Web application » sont des attaques portant sur les applications web et les services web. Elles exploitent le plus souvent de mauvaises configurations ou des vulnérabilités dans les composants ou dans l'infrastructure.

Les attaques les plus fréquentes sont des injections de code SQL, des injections PHP, des Local File Inclusion (FLI), des cross site scripting (XSS)...

Les bons réflexes sont notamment :

- d'établir une politique de sécurité concernant le développement et la mise en production des applications ;
- de recourir à des mécanismes d'authentification et d'autorisation répondant aux règles de l'art ;
- d'installer un web application firewalling (WAF) permettant de vérifier les données HTML, HTTPS, SOAP, XML-RPC ;
- de filtrer le trafic en vérifiant les performances sur les différents canaux (intranet, internet, mails...) ;
- de scanner régulièrement et faire des tests de détection d'intrusion.

Pour en savoir plus, vous pouvez notamment consulter :

- le site securitymadein.lu
- le livre blanc du CERT.eu

4. Phishing

Le Phishing (ou tentative d'hameçonnage) est un type d'attaque qui prend la forme d'un mail alarmant (suppression de votre compte, facture à payer avant saisie...) semblant provenir d'une entreprise connue et de confiance (banques, pouvoirs publics, fournisseurs de services...).

L'objectif est de soutirer des informations personnelles à l'utilisateur (données bancaires, nom des comptables de l'entreprise...).

Parfois, le courrier électronique contenant une reproduction du logo de l'entreprise usurpée envoie la victime sur un site web qui a également été usurpé ou invite la victime à ouvrir une pièce attachée infectée. L'e-mail et le site semblent authentiques et dans certains cas l'adresse URL est masquée de telle sorte qu'elle semble correcte.

© weerapat1003 - Fotolia.com

Parmi les bons réflexes, citons notamment :

- organisation d'une campagne de sensibilisation des employés concernant le phishing (voir kit de sensibilisation à destination des PME) ;
- filtrage des e-mails ;
- vérification DNS ;
- détection et suppression des pièces attachées infectées ;
- détection des caractéristiques des liens URL malicieux ;
- détection des fraudes et anomalies sur le réseau ;
- authentification multifactorielle obligatoire pour tous les éléments critiques (gestion des comptes bancaires...).

Vous pouvez également dénoncer la tentative de phishing via le lien suivant : suspect@safeonweb.be.

En dénonçant l'adresse d'un site de phishing, chaque site fera l'objet d'une validation et s'il s'agit bien d'une tentative de phishing, les browsers seront tenus au courant et bloqueront les adresses problématiques dans les navigateurs. Vous contribuerez ainsi à diminuer l'impact de ce type de tentative en empêchant que d'autres internautes soient à leur tour victimes de la fraude.

Vous pouvez également vérifier une adresse URL via cet outil

5. SPAM

Il s'agit d'un type d'attaque ayant le plus souvent recours à un botnet pour lancer massivement des e-mails malicieux transportant des malwares (fichiers exécutables...).

Les spams ont gagné en qualité en 2017, par exemple en combinant des informations pour mieux piéger leurs victimes tout en ayant recours à certaines techniques afin d'éviter les filtres anti-spams.

La majorité des spams proposent un contenu relevant de l'une des catégories suivantes :

- contenu adulte (à caractère sexuel) ;
- lettres en chaine ;
- santé et pseudo – produits pharmaceutiques ;
- IT et pseudo virus ayant infecté votre système ;
- bancaires (demandes « urgentes » impliquant le transfert de données bancaires) ;
- fausses victoires de loterie ;
- lettres nigérianes (demande d'assistance dans le mouvement/transfert de fonds monétaires étrangers) ;
- éducation (promesses de bourses dans de grandes universités...).

Parmi les bons réflexes, citons notamment :

- dresser la liste des spammers connus[1] et bloquer tout mail provenant de leur botnet ;
- utiliser des filtres adaptés (filtre de réputation, de contenu, RBL, anti-spam, anti-malware...) ;
- bloquer les fichiers exécutables (.exe) attachés dans les e-mails ;
- empêcher l'exécution automatique de codes, macros, graphiques, etc. ;
- sensibiliser les employés (ne pas ouvrir les pièces attachées de mails suspects...) ;
- scanner et filtrer les mails avec pièces attachées.

1 Une liste des 10 spammers mondiaux les plus connus est régulièrement mise à jour et gratuitement disponible sur le site de SPAMHAUS : https://www.spamhaus.org/statistics/spammers/

6. DDoS

Les attaques par déni de service (Distributed Denial of Service) sont menées contre un site web ou un serveur et ont pour objectif de l'empêcher de continuer à fonctionner correctement et d'empêcher les utilisateurs légitimes d'un service de l'utiliser de manière normale. Pour être efficace, ce type d'attaque repose le plus souvent sur un grand nombre d'objets connectés infectés (botnet). En raison du nombre gigantesque d'informations, le site web ou le serveur attaqué ne peut plus traiter les innombrables requêtes et n'est dès lors plus accessible.

Le nombre grandissant d'objets connectés (IoT) qui peuvent être autant de points de vulnérabilité permettant d'être contrôlés par des cyberattaquants laisse malheureusement présager que ce type d'attaques pourrait devenir de plus en plus fréquent.

Parmi les bons réflexes, citons notamment :

- prévoir une politique de sécurité et un Incident Management Plan avec un point concernant les attaques DDoS ;
- avoir de préférence recours à un fournisseur d'accès à internet (FAI ou ISP) qui implémente des mesures de protection contre les attaques DDoS ;
- avoir recours à des outils spécifiques : Firewall based, Access Control Lists (ACLs), Load-balancer, IPS/WAF, Intelligent DDoS mitigation systems (IDMS), Cloud-based DDoS mitigation service...
- contrôles et tests sur les mesures prises par l'entreprise et sur ses capacités de réaction ;
- prévoir un Intrusion Prevention System (IPS) car certaines attaques DDoS peuvent masquer une tentative d'intrusion.

Pour en savoir plus, consultez :

- le livre blanc du Cert.be DDoSProactive and Reactive measures
- la page Attaques DDos : comment se protéger
- le livre blanc du Cert.eu : DDoS : Overview and Response Guide (2017)

7. Ransomware

Un ransomware est un programme malveillant qui encrypte les données figurant sur l'appareil infecté tout en promettant de restituer les données moyennant paiement d'une rançon (en bitcoins).

Pour plus d'infos, consultez :

- le site No more ransom !
- le site Ransomfree.cybereason

Parmi les bons réflexes, citons notamment :

- disposer d'une bonne gestion des back-up (copies de sauvegarde, de préférence stockée ailleurs) ;
- disposer d'un antivirus efficace ;
- mettre à jour son système d'exploitation (OS) et ses applications ;
- activer la fonction « Afficher l'extension des noms de fichiers » dans la configuration du système d'exploitation (OS) de vos ordinateurs. Cela vous aidera à repérer plus facilement les fichiers potentiellement malveillants. Méfiez-vous des extensions telles que « .exe », « .vbs » et « .scr ». Les escrocs peuvent utiliser différentes extensions pour camoufler un fichier malveillant en vidéo, photo ou document (comme hot-chics.avi.exe ou doc.scr) ;
- si vous découvrez un processus scélérat ou inconnu sur votre machine, déconnectez-la immédiatement de l'internet ou de tout autre connexion réseau (comme le wi-fi de votre entreprise), cela empêchera l'infection de se propager en attendant l'intervention d'une équipe technique.
- penser à consulter les sites spécialisés qui peuvent vous proposer de bons conseils et outils en matière de prévention ainsi qu'en matière de nettoyage des appareils infectés
  - » https://www.nomoreransom.org/
  - » https://ransomfree.cybereason.com/

Pour en savoir plus, consultez également le guide Ransomware. How to protect and respond du CERT.

© zephy_P - Fotolia.com

8. Botnets

Un botnet est un réseau d'objets connectés (« armée d'appareils zombies ») qui sont utilisés – souvent à l'insu de leurs propriétaires – pour attaquer des sites web ou des serveurs d'entreprises et d'organisations en bombardant les victimes de requêtes ou de malwares (voir DDoS, e-mails avec pièces attachées malicieuses…).

N'importe quel objet connecté à internet peut faire partie d'un botnet. Le processus est le suivant : un programme malveillant contamine un objet connecté à internet mais reste invisible sur celui-ci. Il attend un ordre des cybercriminels. A partir du moment où les cybercriminels ont contaminé suffisamment d'objets connectés, ils donnent l'ordre aux objets infectés de bombarder un site web ou un serveur déterminé. Des botnets peuvent aussi être loués à d'autres cybercriminels en passant sur le Dark web.

Parmi les bons réflexes, citons notamment :

- installation et configuration du réseau et firewall ;
- analyse des performances du trafic sur l'ensemble des canaux utilisés (intranet, internet, e-mails…) ;

- installation de black-list des adresses IP infectées détectées[2] ;
- installation d'un Botnet Sinkholing (la détection d'une attaque via botnet permet de rediriger les attaques vers un serveur martyr qui servira à collecter des données sur l'attaque lancée).

9. Insider Threat

L'insider threat ou « menace de l'intérieur » relève le plus souvent de la négligence ou d'une simple maladresse mais il peut également s'agir d'un acte malveillant de la part de l'un de vos (ex)employés.

Parmi les bons réflexes, citons notamment :

- comptes administrateurs limités et implémentation d'un Privileged Identity Management (PIM) ;
- mise en place d'un Identity and Access Management (IAM) (définition des rôles) ;
- sensibilisation de vos employés au sujet de ce qu'ils peuvent/ne peuvent pas faire avec les outils de travail qui leur sont confiés ;
- politique de sécurité prévoyant un point particulier en cas de licenciement de l'un/de plusieurs de vos employés ;
- mise en place d'une gouvernance des risques sur la base des différentes fonctions ;
- outils d'analyse des données ;
- monitoring des usagers (abus des droits fixés) et audit régulier.

10. Dommage physique, perte ou vol

Bien qu'il ne s'agisse pas à proprement parler d'un risque cyber, les dommages physiques représentent une menace importante.

Il peut s'agit de la perte/du vol de clefs USB sur lesquelles d'importantes informations non cryptées ont été stockées, de vols de serveurs (salle non protégée), de vols de GSM sur lesquels figurent des dossiers ou des e-mails contenant des informations importantes, de non- renouvellement des contrats de maintenance avec pour conséquence des serveurs en panne, des batteries de secours qui ne prennent pas le relais en cas de rupture de courant...

2 Une liste des principaux botnets mondiaux est régulièrement mise à jour et gratuitement disponible sur le site de SPAMHAUS.

Parmi les bons réflexes, citons notamment :

- crypter toutes les informations devant se trouver sur des supports mobiles (GSM, clefs USB...) ainsi que sur votre réseau ;
- tenir un tableau des contrats de maintenance avec retroplanning afin de les renouveler endéans les temps ;
- tenir un inventaire des supports autorisés (et interdire les autres supports) ;
- établir des procédures pour les employés afin qu'ils sachent comment réagir en cas de vol de matériel (PC, GSM, USB...) et sensibiliser votre personnel ;
- si besoin, se faire couvrir par une assurance adaptée pour le vol et les risques cyber.

Pour en savoir plus, vous pouvez notamment consulter CIRCLean - USB key sanitizer.

Pensez à consulter les sites plus spécialisés dans les alertes techniques afin d'être tenu au courant des dernières tendances en ce qui concerne les vulnérabilités et les menaces :

ENISA

CERT.be

US-CERT

CASES

economie
SPF Economie, P.M.E., Classes moyennes et Energie

Rue du Progrès 50
1210 Bruxelles
N° d'entreprise : 0314.595.348
https://economie.fgov.be