

77 % des entreprises totalement impuissantes face aux cyberattaques



Pénurie de compétences et manque d'investissements : les entreprises sont non seulement vulnérables aux attaques, mais aussi impuissantes pour les résoudre seules. Décryptant les tendances de ces trois dernières années dans le monde, un rapport de NTT Com Security souligne le peu de progrès réalisés dans ce domaine, et note même un recul...

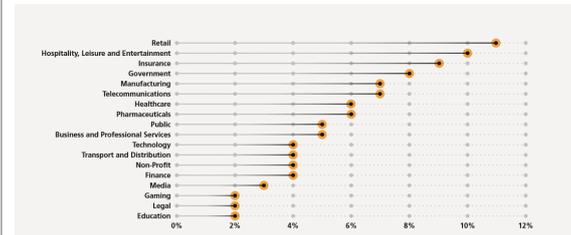


Le GTIR (« Global Threat Intelligence Report ») analyse une énorme masse de données issues de 24 centres d'opérations de sécurité (SOC), sept centres R&D, 3 500 milliards de logs et 6,2 milliards d'attaques. Ces résultats sont donc particulièrement intéressants pour suivre l'état des menaces dans le monde. Son édition 2016, qui décrypte les tendances de ces trois dernières années souligne le peu de progrès réalisés par les entreprises dans leur lutte contre les menaces, et note même une légère hausse du nombre d'entre elles mal préparées qui s'élève à 77 %. Face à des attaques d'envergure, elles doivent le plus souvent solliciter une intervention extérieure. Seules 23 % des organisations seraient donc en mesure de se défendre efficacement contre des incidents de sécurité majeurs.

Le retail le plus touché par les incidents

Après des années passées en tête des secteurs les plus touchés dans les précédents rapports GTIR, la finance cède sa place à la grande distribution qui enregistre 22 % des interventions sur incidents (contre 12 % l'année passée) de NTT Com Security. La grande distribution a été particulièrement exposée aux attaques de spear phishing. Parce qu'elles brassent d'importants volumes de données personnelles, dont des informations bancaires, les organisations de ce secteur constituent une cible particulièrement attractive, et ce au point d'enregistrer le plus fort taux d'attaques par client. Le secteur financier a représenté 18 % des interventions.

En 2015, le groupe NTT a également noté une augmentation des attaques à l'encontre du secteur de l'hôtellerie, des loisirs et du divertissement. Tout comme la grande distribution, ce secteur draine aussi de gros volumes d'informations personnelles, y compris des données de cartes bancaires. De même, le niveau relativement élevé des transactions dans le milieu (hôtels, stations touristiques...) suscitent la convoitise des attaquants. Avec sa palette de programmes de fidélité, l'hôtellerie est une vraie mine d'informations personnelles. Plusieurs violations de sécurité ont d'ailleurs défrayé la chronique en 2015 : Hilton, Starwood ou encore Hyatt.



Les attaques par secteur – 2015

Hausse de 17 % des menaces internes

A quels types d'incidents NTT Com Security a-t-il été confronté ? Les violations de sécurité ont représenté 28 % des interventions en 2015, contre 16 % en 2014. Un grand nombre d'incidents concernaient des vols de données et de propriété intellectuelle. Les menaces internes ont connu de leur côté une véritable envolée, passant de seulement 2 % en 2014 à 19 % en 2015. Elles résultent le plus souvent d'une utilisation abusive des données et ressources informatiques par des salariés ou prestataires externes.

En 2015, 17 % des interventions de NTT Com Security se sont produites sur des attaques par spear phishing, alors qu'elles représentaient moins de 2 % auparavant. Basées sur des tactiques sophistiquées d'ingénierie sociale, comme l'utilisation de fausses factures, ces attaques visaient principalement des dirigeants et autres personnels de la fonction comptabilité-finance.

Enfin, le GTIR 2016 a enregistré un recul des attaques #DDoS par rapport aux années précédentes. Elles ont reculé de 39 % par rapport à 2014. Le rapport attribue cette baisse aux investissements réalisés dans les outils et services de défense contre ce type d'agression.

A noter cependant une augmentation des cas d'extorsion, où les victimes d'acquiescent d'une rançon pour lever les menaces ou stopper une DDoS en cours.

Top 10 External Vulnerabilities		Top 10 Internal Vulnerabilities	
Outdated PHP Version	8%	Outdated Java Version	51%
Cross Site Scripting (CSS/XSS)	7%	Outdated Adobe Flash Player	11%
Outdated Apache Web Server	7%	Outdated Adobe Reader and Acrobat	5%
SSL/TLS Information Disclosure	6%	Outdated Microsoft Windows	3%
Web Clear Text Username/Password	5%	Outdated Microsoft Internet Explorer	3%
Weak SSL/TLS Cipher/Certificate	5%	Outdated Mozilla Firefox	2%
Outdated Apache Tomcat Server	4%	Outdated Microsoft Office	1%
Weak/No HTTPS cache policy	4%	Outdated Linux Kernel	1%
Cookie without HTTPOnly attribute set	3%	Outdated Novell Client	1%
SSL Certificate Signed using Weak Hashing Algorithm	3%	Outdated OpenSSH Version	1%

Top 10 des vulnérabilités internes et externes – 2015. Parmi l'ensemble des vulnérabilités externes identifiées, le top 10 compte pour 52 % des cas recensés. Les 48 % restants étaient composés de milliers de vulnérabilités. Parmi l'ensemble des vulnérabilités internes identifiées, le top 10 compte pour 78 % des cas recensés. Ces 10 vulnérabilités internes étaient directement liées à la présence d'applications obsolètes sur les systèmes visés.

Article original de Juliette PAOLI



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique;
- Formations et conférences en cybercriminalité;
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Cyberattaques : 77 % des entreprises totalement impuissantes | Solutions Numériques