CHUBB®

Les frontières du risque technologique

Sensibilisation au risque cybernétique pour les entreprises ICT

CHUBB®

Sensibilisation au risque cybernétique pour les entreprises ICT

Contributors

Barry Schütte
Manager Industry Practices Benelux, Chubb

Wouter Wissink
Senior Principal Cyber Risk Engineer and Technology Industry Practitioner, Chubb

La cybersécurité est un domaine de risque qui requiert une énorme attention, notamment dans la mesure où les coûts mondiaux liés à la cybercriminalité devraient atteindre près de 10 500 milliards de dollars chaque année d'ici 2025, selon Cybersecurity Ventures. Les entreprises ICT sont particulièrement vulnérables face aux pirates informatiques, leur rôle d'intermédiaires faisant d'elles une cible pour diffuser des logiciels malveillants ou des rançongiciels auprès de plusieurs entreprises à la fois.

Les attaques Kaseya et SolarWinds sont deux exemples très connus des dégâts que peuvent causer des entreprises criminelles de plus en plus sophistiquées. « Les pirates informatiques organisés sont de plus en plus motivés par la monétisation de leurs activités, le rançongiciel constituant désormais la principale cybermenace », avertit l'Agence de l'Union européenne pour la cybersécurité.

La lutte contre la cybercriminalité nécessite une solide infrastructure de sécurité et une attention continue à l'égard des contrôles. Les risques peuvent être considérablement atténués en respectant certaines mesures de cyber-hygiène. Cependant, les attaques devenant de plus en plus ciblées et avancées, que doivent faire les entreprises ICT pour se protéger ?

Risques fréquents

Ces entreprises sont confrontées à deux risques essentiels étroitement liés : les attaques contre leurs propres environnements et celles qui nuisent à leurs clients. Une cyberattaque ciblant un distributeur ou un développeur de logiciels pourrait conduire au vol de données confidentielles, qui pourraient ensuite être détournées par des pirates informatiques pour accéder directement à l'environnement d'un client. Si une entreprise ICT fait l'objet d'une attaque par rançongiciel, elle peut se trouver dans l'incapacité de fournir les services d'assistance essentiels à ses clients. De même, un logiciel compromis par une porte dérobée peut être vendu à son insu à des clients, facilitant ainsi une attaque contre des centaines voire des milliers d'entreprises.

« Les cybercriminels peuvent également causer du tort en accédant aux clients par l'intermédiaire des Managed Service Providers (MSP ou fournisseurs de services d'infogérance) », avertit Wouter Wissink, Senior Principal Cyber Risk Engineer and Technology Industry Practitioner chez Chubb.

« Les répercussions commerciales, financières et de réputation pour les entreprises ICT peuvent être énormes », déclare Barry Schütte, Industry Practices Manager chez Chubb. « Les entreprises inquiètes risquent d'aller chez un concurrent, par exemple, impactant ainsi le bénéfice net », explique-t-il.

Des décisions commerciales difficiles à prendre

Quels enseignements pouvons-nous tirer des crises Kaseya et SolarWinds ? Dans le cas de la multinationale américaine Kaseya, en juillet 2021, des pirates informatiques ont exploité une faille de son logiciel Virtual System Administrator (VSA) fourni à des MSP et à des équipes informatiques, lors d'une attaque zero-day.

Liste de contrôle des bonnes pratiques en matière de cyber-hygiène

- Pouvez-vous identifier les risques auxquels votre entreprise et vos clients sont confrontés ?
- Savez-vous quoi faire pour prévenir ces risques ?
- Avez-vous mis en place des mesures solides pour détecter le risque cybernétique ?
- Avez-vous établi un plan précis d'intervention en cas de piratage informatique ?

« En leur qualité d'intermédiaire, les MSP sont confrontés à un véritable risque cybernétique »

« Cette phase d'entre-deux est très difficile à protéger », explique Wissink. « Les éditeurs de logiciels ont besoin d'une semaine, voire plus, pour résoudre ce type de problème et, au cours de cette période, ces développeurs sont très exposés. »

La perte subie par Kaseya a été limitée à près de 50 clients, mais jusqu'à 1 500 entreprises intervenant en aval à l'échelle mondiale auraient également été frappées par le rançongiciel.

L'exposition à ce genre d'attaques s'accélère. En 2021, les failles « zero-day » auraient doublé, selon un rapport de Rapid7. « Il s'agit du domaine de risque le plus critique, car il est très difficile à gérer » explique Wissink. Il encourage vivement les entreprises touchées à prévenir leurs clients le jour même du piratage d'un système, à mettre rapidement les systèmes hors ligne et à tenir les clients informés.

« Cela peut s'avérer très difficile pour certaines entreprises », prévient-il. « Cela revient à dire à vos clients que votre modèle commercial n'est plus fiable et qu'ils doivent se déconnecter. »

Tactique de porte dérobée

Six mois avant l'incident de Kaseya a eu lieu l'attaque contre la chaîne logistique, baptisée Solarigate, au cours de laquelle des cybercriminels ont intégré un logiciel malveillant aux mises à jour dans le système logiciel Orion de SolarWinds - largement utilisé par des entreprises de gestion des ressources informatiques.

« Les pirates informatiques ont réussi à accéder à l'environnement de développement », déclare Wissink. Le logiciel malveillant s'est propagé sans être détecté dans le cadre d'une mise à jour logicielle régulière pour les clients, créant ainsi une « porte dérobée » permettant d'accéder à leurs systèmes informatiques. Environ 18 000 clients ont été exposés, dont des agences gouvernementales américaines et des marques internationales. Selon Wissink, « l'adoption de mesures élémentaires en matière de cyber-hygiène aurait pu empêcher cette attaque ».

Tendances émergentes

Quelles tendances les assureurs voient-ils émerger à l'heure actuelle ? « Les entreprises améliorent leurs propres niveaux de protection », déclare Schütte, « les cybercriminels ciblent donc de plus en plus les prestataires et les fournisseurs. En leur qualité d'intermédiaire, les MSP sont confrontés à un véritable risque cybernétique et la croissance soutenue sur ce marché s'est accompagnée d'une hausse des sinistres ».

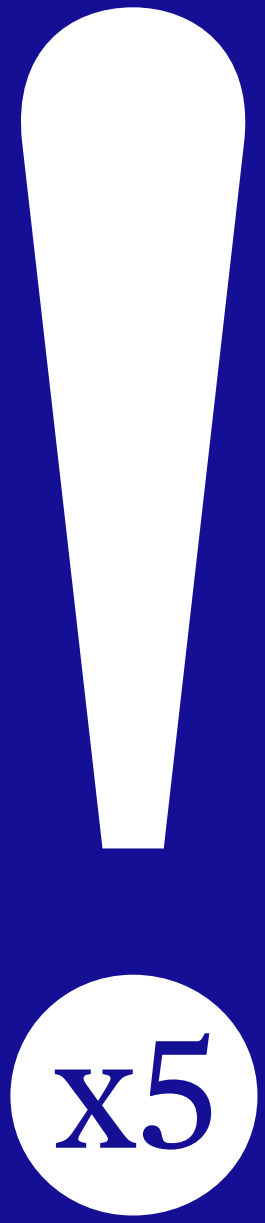
« Les environnements PaaS (Platform as a Service) et SaaS (Software as a Service) sont également plus exposés », ajoute-t-il. « Le profil de risque a donc considérablement augmenté avec le délaissement des systèmes logiciels sur site au profit des modèles commerciaux basés dans le Cloud ou sur une plateforme. »

L'obligation de diligence constitue un autre domaine de risque émergent. « Dans le cadre d'une relation fournisseur/client, une entreprise ICT est généralement considérée comme l'experte », explique Schütte. « Ses obligations vont souvent au-delà des dispositions contractuelles, ce qui signifie que les risques en matière de responsabilité s'aggravent. » Un prestataire a conseillé à un client de prendre des mesures de sécurité supplémentaires, mais a omis de documenter son conseil. Lorsque le client a subi une attaque par rançongiciel et a ensuite porté plainte, l'entreprise ICT a été jugée responsable.

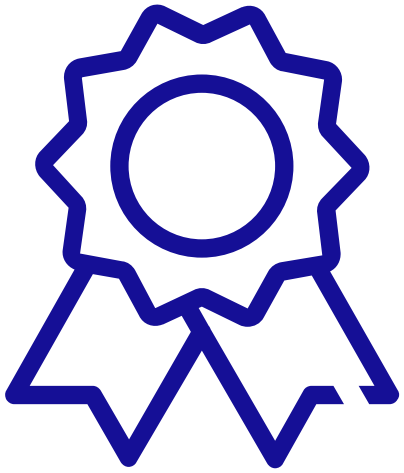
Par conséquent, comment atténuer ces risques en adoptant de bonnes pratiques en matière de cyber-hygiène ? Découvrons les bonnes pratiques à adopter par les entreprises ICT autour de quatre piliers essentiels : l'identification, la prévention, la détection et la réaction.

Identification des risques

« Il suffit d'assurer une gestion rigoureuse des risques pour établir le risque cybernétique », affirment Wissink et Schütte. Les entreprises ICT doivent identifier avec précision les produits et les services qu'elles fournissent pour estimer ceux qui sont susceptibles d'entraîner un risque. Conçoivent-elles des logiciels ? Distribuent-elles des logiciels ? Exercent-elles une activité de MSP ? Conservent-elles des mots de passe pour leurs clients ?



« Au lieu d'un risque majeur, nous observons désormais cinq grands risques, de sorte que le risque pour les entreprises ICT est cinq fois supérieur à ce qu'il ne l'était il y a 10 ou 15 ans »



Un Système de Management de la Sécurité de l'Information (SMSI) permet aux entreprises de cerner ces éléments. Ce cadre géré de manière centralisée leur permet de gérer, surveiller et revoir leurs pratiques en matière de sécurité de l'information.

Bien que les développeurs de logiciels déploient généralement « des efforts considérables » pour concevoir un produit sécurisé, Wissink déclare qu'ils négligent souvent d'accorder une protection similaire à leurs propres environnements. À titre d'exemple, les clients sont régulièrement invités à télécharger le logiciel depuis un site Web qui n'est pas correctement protégé.

Renforcement des défenses

La lutte contre les cyberattaques nécessite, a minima, de prendre des mesures d'hygiène standard, dont l'authentification multifactorielle, une formation de sensibilisation adaptée à l'intention du personnel, des pares-feux, l'analyse des e-mails de phishing et le filtrage des sites Web.

« Néanmoins, les entreprises ICT doivent vraiment adopter les pratiques exemplaires, compte tenu de l'impact potentiel accru des pertes subies à la suite d'un événement généralisé et du renforcement des responsabilités au titre de l'obligation de diligence », conseille Wissink. Selon lui, les entreprises ont besoin d'un système de PAM (Privileged Access Management ou gestion des accès à privilèges). L'outil PAM préserve les identités, grâce à un accès privilégié ou des capacités dépassant celles accordées aux utilisateurs réguliers. Il est particulièrement important pour les MSP, dont de nombreux collaborateurs ont accès à plusieurs programmes par le biais d'un progiciel central.

« Les développeurs de logiciels doivent également isoler leur réseau et le protéger à l'aide d'outils supplémentaires uniquement accessibles aux développeurs » recommande Wissink. « Cet environnement de développement ne doit pas avoir de connexion automatique au reste de l'entreprise. »

Parmi les autres bonnes pratiques de gestion interne visant à réduire l'exposition et à contribuer à la continuité des activités figurent notamment le test régulier des sauvegardes et leur stockage hors ligne ainsi qu'une attention particulière au chiffrement des mots de passe et autres données. L'embauche d'un responsable dédié à la sécurité informatique est également un choix judicieux.

« Les entreprises doivent non seulement protéger ces données, mais également conclure un accord contractuel satisfaisant avec le client concernant les modalités de conservation et de traitement de leurs données », déclare Schütte.

Néanmoins, la prévention ne se réduit pas à mettre en place des mesures techniques de prévention. Il s'agit également de communication, via la mise en place d'accords contractuels de niveau de service et de contrats relatifs à la protection des données. « Un prestataire informatique, en particulier un MSP, est tenu, selon le principe de l'obligation de diligence, d'avertir et d'informer leurs clients du niveau de protection éventuellement faible d'un environnement client spécifique », ajoute Wissink. « Les clients doivent être informés par écrit et, pour se prémunir contre les risques de responsabilité, il convient également de garder une trace de cette information. »

Selon Schütte, bon nombre d'entreprises ICT sont en retard dans la mise à jour de leurs politiques de développement sécurisé. Cela inclut notamment les tests d'intrusion et les tests de vulnérabilité ainsi que la revue des codes et la formation au codage (le Top 10 de l'OWASPpeut s'avérer utile).

« Les développeurs de logiciels qui conçoivent des logiciels non critiques ne doivent pas négliger la nécessité de ces politiques », conseille-t-il.

« Face aux menaces actuelles, chaque entreprise est une cible », avertit Wissink.

Points importants à retenir

- **Les attaques ciblant les MSP constituent la** principale tendance émergente en matière de sinistres
- **Les entreprises ICT doivent mieux** maîtriser les failles « zero-day »
- **Les risques liés à l'obligation de diligence sont** en hausse et doivent faire l'objet d'une attention particulière
- **Un Système de Management de la Sécurité de** l'Information (SMSI) peut faciliter l'identification du risque
- **Utilisez un outil PAM (Privileged Access** Management) pour contribuer à contrer les pirates informatiques
- **Isolez votre système logiciel du reste de** l'entreprise
- **La communication avec les clients constitue** également un élément essentiel de la cyber-prévention
- **Mettez en œuvre des politiques adéquates de** développement sécurisé
- **La mise en place d'un système de surveillance** du réseau (suivi 24 h/24, 7 j/7) est une idée judicieuse
- **Ne négligez pas les plans formels d'intervention** en cas d'incident et de continuité des activités
- **N'oubliez pas de tester régulièrement vos** sauvegardes et de les stocker hors ligne

Détection des cyber infractions

Les logiciels de surveillance et de détection tels que l'EDR (Endpoint Detection and Response) sont indispensables pour les entreprises ICT, tout comme les pares-feux efficaces ou un système de surveillance du réseau, suivi 24 h/24, 7 j/7 par un centre opérationnel de sécurité interne ou externe. « Une fois qu'un pirate informatique s'est infiltré dans un système, il est primordial de le détecter à temps » souligne Wissink.

« Éteindre l'incendie »

Wissink et Schütte s'accordent à dire que la mise en place d'un plan précis d'intervention en cas d'incident constitue l'un des éléments indispensables pour qu'une entreprise puisse faire face aux cyberattaques. Une planification préalable minutieuse aidera une entreprise à réagir de manière adéquate et rapide, en cas de piratage informatique. Pour un éditeur de logiciels, ce plan ne se limite pas à son propre environnement informatique ; il doit également inclure une politique de communication avec les clients et de gestion de crise. D'après leur expérience, bon nombre d'entreprises ne sont pas préparées. « La plupart du temps, elles ne savent pas quoi faire », déclare Schütte.

En cas de violation des systèmes informatiques, les entreprises doivent s'assurer que les services sont sécurisés et remis sur pied dès qu'ils sont viables, et qu'elles sont en mesure de servir leurs clients avec efficacité dans l'entre deux.

Même si l'avenir du risque cybernétique à l'heure du numérique peut sembler inquiétant, l'absence de mesures préventives pour protéger votre entreprise reviendrait en quelque sorte à laisser en permanence votre porte d'entrée grande ouverte en espérant que rien ne soit volé. Il serait bien plus avisé de vous renseigner sur la cyber-hygiène et de mettre en place les éléments appropriés permettant de protéger vos clients et vous-mêmes.

Principaux contacts

Barry Schütte
Manager Industry Practices Benelux, Chubb
bschutte@chubb.com

Wouter Wissink
Senior Principal Cyber Risk Engineer and Technology Industry Practitioner, Chubb
wwissink@chubb.com

Fiorella Perrone
Underwriter, Financial Lines, Suisse Romandie
fiorella.perrone@chubb.com

Chubb. Insured.℠

Chubb Versicherungen (Schweiz) AG / Chubb Insurance (Switzerland) Limited / Chubb Assurances (Suisse) SA. Bärengasse 32, 8001 Zürich, T + 41 43 456 76 00, www.chubb.com/ch-fr

CH-FR8221-07/22