TRIGONE
OSER S'ENGAGER

PART OF THE NRB GROUP

PROTÉGER
SES DONNÉES
POUR PROTÉGER
SON ENTREPRISE

LA CYBERSÉCURITÉ EST UN ENJEU MAJEUR POUR LES SECTEURS PRIVÉ ET PUBLIC, D'AUTANT QUE LES ATTAQUES N'ONT JAMAIS ÉTÉ AUSSI NOMBREUSES.

« *Un ordinateur en sécurité est un ordinateur éteint. Et encore…* »

Cette citation de Bill Gates date du début du millénaire. Il y a vingt ans, la cybersécurité était déjà un sujet brûlant. Aujourd'hui, cette problématique continue de se propager à une vitesse impressionnante, notamment à la suite des derniers événements qui ont secoué le monde au cours des dernières années. « *Le confinement lié au coronavirus et la guerre en Ukraine ont grandement contribué à une recrudescence des attaques en ligne* », confirme Vincent Ceriani, Head of Cyber Risk Services du Groupe NRB, dont fait partie l entreprise Trigone.

Les exemples de vols de données ne manquent pas. Chaque semaine, un nouveau cas est dévoilé et les conséquences peuvent être désastreuses. Les grandes villes, les hôpitaux ainsi que des entreprises sont les cibles de hackers, toujours à la recherche d'une victime pour lancer leur attaque. « *Les plus petites sociétés craignent de perdre de l'argent ou de devoir stopper leur production pendant de longues semaines. Les grandes entreprises ont peur de voir leur réputation se fragiliser* », explique Lorenzo Bernardi, Head of Security Services de NRB.

Les menaces sont connues, tout comme la nature des attaques. « ***Le hacking et le ransomware sont les deux options à la mode***, *si je puis dire. Par exemple, deux de nos clients ont déjà subi un hacking lors des trois premiers mois de cette année* », dit Lorenzo Bernardi. « *Des personnes malintentionnées peuvent prendre possession de données parce que les mises à jour n'ont pas été effectuées régulièrement. Pourtant, c'est une simple action à réaliser mais de trop nombreuses entreprises n'ont pas encore ce réflexe. Tout le monde parle de la cybersécurité mais en réalité, on remarque qu'il y a un réel manque de connaissances dans ce domaine.* »

L'expertise du Groupe NRB est reconnue dans les secteurs privé et public. Pour preuve, le chiffre d'affaires des activités en matière de cybersécurité a été multiplié par six au cours des quatre dernières années et les trois premiers mois de l'année 2023 ont déjà permis de dépasser la valeur des contrats de l'année 2022. « *Ce n'est pas étonnant car il y a de plus en plus de systèmes connectés, tout est informatisé et les organisations criminelles ont bien compris l'intérêt financier qu'elles pouvaient en tirer* », décrit Vincent Ceriani.

LE PROBLÈME : LE MANQUE DE CONNAISSANCES

La cybersécurité est un sujet régulièrement abordé dans les médias et les entreprises. Pour autant, **mettre en place une bonne stratégie de défense n'est pas aussi simple** qu'il n'y paraît tant tout paraît nouveau. « *Prenons l'exemple du télétravail qui s'est développé durant le Covid. Des solutions de travail à distance ont été lancées pour permettre aux employés de travailler dans les meilleures conditions depuis leur domicile. Malheureusement, certains n'ont pas opté pour une authentification forte, en se passant de demander une deuxième authentification via le GSM. Dans ces conditions, le hacker n'a besoin que d'un nom et d'un mot de passe pour réussir son piratage. Une fois qu'il pénètre dans le système de l'entreprise, toutes les données sont à sa disposition* », continue Vincent Ceriani.

Obtenir ces données peut se faire en un seul clic. « *Imaginons : un membre du secrétariat, trop peu sensibilisé à la sécurité, ouvre un e-mail qui lui promet de gagner un super téléphone s'il donne son nom, son numéro de téléphone et son mot de passe. Le hacker récupère donc ces données et peut entreprendre toutes les actions qu'il souhaite. Un client m'a récemment expliqué qu'un pirate avait stoppé l'envoi des e-mails de facturation, les avait édités pour y mentionner son numéro de compte et les avait ensuite renvoyés aux clients. Je vous laisse imaginer les conséquences…* »

Les entreprises sont responsables des données personnelles dont elles disposent, qu'elles concernent leur personnel ou leurs clients. Ce règlement général sur la protection des données (GDPR) a été voté en avril 2016 mais son contenu est encore trop méconnu du grand public. « *J'ai parfois l'impression que certains découvrent cette loi. Si un hacker vole des données, c'est la société qui en sera tenue responsable. Récemment, un client m'a expliqué donner une feuille de papier regroupant les informations de sa clientèle et l'horaire de tournée à ses livreurs. Cela ne pose pas de problème à proprement parler, sauf si les livreurs laissent la feuille chez le dernier client car ils n'en ont plus besoin. Dans ce cas, un client se retrouve avec les données de l'ensemble des autres clients (adresse, numéro de téléphone…)* », explique Vincent Ceriani.

— **Vincent Ceriani**
Head of Cyber Risk Services du Groupe NRB

DES TESTS DE PÉNÉTRATION OFFERTS PENDANT LA GUERRE EN UKRAINE

La sécurité des données est un enjeu majeur dans la société. Malheureusement, tout le monde ne peut se permettre de réaliser un audit via un test de pénétration. Le Groupe NRB a offert ses services à des ASBL et écoles au début de la guerre en Ukraine, moment choisi par les hackers pour multiplier leurs attaques. « *Il était important de mettre nos compétences au service de la population et du pays. Nous avons donc décidé de libérer du temps et des collaborateurs pour prêter main-forte à ceux qui en avaient le plus besoin* », note Lorenzo Bernardi.

LE GROUPE NRB, UN EXPERT RECONNU EN SÉCURITÉ

Le Groupe NRB investit dans la cybersécurité et propose un service complet à ses clients. **Nos experts peuvent intervenir tant sur le plan légal et compliance que technologique**. « *Cette combinaison représente, à nos yeux, la réussite d'un plan de sécurité. Les associer étroitement permet de gagner cette bataille* », affirme Lorenzo Bernardi.

Pour répondre aux besoins de ses clients, le Groupe recrute en permanence des spécialistes en matière de sécurité. Une véritable formation leur est offerte. « *Un informaticien ne peut pas sécuriser toute une entreprise, c'est un travail à part. Les spécialistes manquent, à un point tel que plusieurs milliers de postes sont vacants. NRB joue un rôle fondamental à ce niveau en recrutant des jeunes collaborateurs pour ensuite les former à tous les enjeux de la sécurité. Nous pouvons presque dire que nous sommes une université à talents* », termine Lorenzo Bernardi.

Notre entreprise dispose d'un catalogue complet pour offrir le meilleur service à ses clients.

1. Le Groupe est actif en matière de prévention contre les attaques venant de l'intérieur et l'extérieur de la société. Les résultats sont déjà importants avec notamment une meilleure protection contre les ransomwares et des campagnes de sensibilisation lancées dans toute la société.

2. Nos experts sont également spécialisés dans le domaine de la détection. Ils procèdent à des audits relatifs à la sécurité de nos clients, notamment via un « piratage éthique ». Sur base des conclusions obtenues, ils établissent une feuille de route d'amélioration de la sécurité.

3. Nous aidons les entreprises victimes d'une cyber attaque à récupérer leurs données et nous leur offrons un support en matière de réglementation (GDPR).

4. Notre Groupe est certifié ISO 27001. Nos experts accompagnent nos clients dans le cadre de leur propre certification ISO 27001.

— **Lorenzo Bernardi**
Head of Security Services de NRB

LES COLLABORATEURS DE TRIGONE FORMÉS À LA SÉCURITÉ

Sans surprise, Trigone et le Groupe NRB sont des cibles pour les hackeurs. « *Une grosse partie de notre trafic internet provient de Russie et de Chine. Aujourd'hui, 25% de ce trafic est encore bloqué automatiquement car nous l'avons identifié comme une potentielle menace. Nous faisons régulièrement face à une augmentation importante du trafic, ce qui est le signe de tentatives d'intrusion. Heureusement, nos systèmes sont protégés efficacement* », explique Mohammed Loucif, en charge de former les collaborateurs de Trigone sur la cybersécurité et le RGPD.

Pour contrer ces menaces, chaque collaborateur est appelé à suivre différents modules traitant de la sécurité. Si une personne préalablement choisie au hasard est piégée, elle bénéficie d'un suivi individuel. « *Chaque collaborateur doit suivre ces formations, selon les besoins de sa fonction. Chaque module se clôture par une évaluation. Nous mettons tout en œuvre pour sensibiliser l'ensemble du personnel à ce risque de hacking* », explique Mohammed Loucif.

CONTACT

INFO@TRIGONE.FR

www.trigone.fr

https://www.linkedin.com/company/trigone-nrb/

Trigone SAS 3, Place Aimé Césaire - 93100 Montreuil, France

info@trigone.fr | +33 (0)1 44 93 21 50

TRIGONE
OSER S'ENGAGER

THE NRB GROUP

bsi. ISO 9001:2015 Quality Management FS 706532 ISO/IEC 27001 Information Security Management IS 706533