Cybersécurité : la confiance à l'ère digitale

Comment protéger votre organisation contre des cybercriminels toujours plus sophistiqués et des atteintes invisibles à la confiance ? C'est l'un des thèmes abordés dans notre Rapport sur les tendances. Dans ce rapport, BDO se projette vers 2030 aux côtés du trendwatcher Tom Palmaerts. Nous montrons comment les entreprises belges peuvent façonner l'avenir avec agilité et confiance. Combiner technologie et bon sens est ici crucial.

Cybersecurity : la confiance à l'ère digitale

La technologie apporte des possibilités inédites, mais rend en même temps les entreprises plus vulnérables que jamais. La cybercriminalité ne tient aucun compte des frontières nationales et est devenue une réalité quotidienne, y compris pour les entreprises belges. Les hackers ne visent pas uniquement les multinationales, mais aussi les PME qui sont souvent moins bien protégées. Les cyberattaques coûtent des milliards dans le monde, mais la plus grande perte est souvent invisible et impossible à chiffrer : la confiance.

« Les cyberrisques restent l'un des dangers les plus sous-estimés pour les entreprises. Malgré une prise de conscience croissante, de nombreuses organisations sous-estiment encore l'impact des fuites de données, des ransomwares et de la faible intégrité des données. Les dommages se limitent rarement aux pertes financières. La réputation, la confiance et la continuité sont en jeu. En outre, une mauvaise qualité des données constitue un risque insidieux. Des données erronées ou incohérentes conduisent inévitablement à de mauvaises décisions et sapent la confiance dans les systèmes et dans le leadership. »

Sam Nelen, Partner Risk Advisory
BDO Belgium

MÉSINFORMATION EN DÉSINFORMATION

Toutes les attaques ne sont pas techniques. Les entreprises sont de plus en plus souvent confrontées à des campagnes de désinformation. Parfois, celles-ci proviennent de concurrents, parfois d'acteurs malveillants. Une telle campagne peut semer la confusion chez les clients et les collaborateurs. Un faux message sur les réseaux sociaux ou un document divulgué peut endommager la réputation d'une entreprise en quelques heures.

TENDANCES EN MATIÈRE DE CYBERPIRATAGE

Les cyberattaques deviennent plus complexes et plus sophistiquées. Le ransomware reste la méthode la plus populaire : les systèmes sont verrouillés et ne sont libérés qu'après paiement. Mais les attaques via la chaîne d'approvisionnement augmentent également, où les hackers ne s'attaquent pas directement à une entreprise, mais à un fournisseur ou un freelance pour ainsi obtenir un accès. Cela montre à quel point les réseaux sont vulnérables : une chaîne n'est aussi solide que son maillon le plus faible.

DEEPFAKES : LA CONFIANCE COMME POINT FAIBLE

La cybercriminalité exploite notre confiance. Un exemple récent vient de Ferrari, où des criminels ont imité la voix d'un dirigeant afin de forcer un paiement urgent. Ce qui a stoppé l'attaque n'était pas une technologie complexe, mais un simple réflexe de bon sens : l'employé a posé une question à laquelle seul le véritable dirigeant pouvait répondre (« Quel livre m'as-tu recommandé hier ? »). L'incident montre que les deepfakes deviennent de plus en plus convaincants, mais aussi que la vigilance et les réflexes critiques restent notre première ligne de défense.

L'ÈRE QUANTIQUE

Une menace supplémentaire se profile encore : le calcul quantique. Des ordinateurs capables de calculer des millions de fois plus vite rendraient inutiles bon nombre de nos méthodes de chiffrement actuelles. Bien que l'ère quantique relève encore de la musique d'avenir, les banques, les gouvernements et les entreprises technologiques s'y préparent déjà. Les entreprises belges ont elles aussi tout intérêt à suivre de près ces évolutions et à rendre progressivement leur sécurité « quantum safe ».

EU CYBER RESILIENCE ACT

Le Cyber Resilience Act de l'UE oblige les entreprises à concevoir des produits et des logiciels plus sûrs et à assumer la responsabilité des vulnérabilités. Cela ressemble à une réglementation supplémentaire, mais cela crée aussi un avantage important : davantage de confiance de la part des clients, des fournisseurs et des investisseurs. Tout comme l'AI Act, cette loi vise à offrir des cadres et de la sécurité juridique. Le CRA n'est pas exhaustif, et sa force dépendra de l'application, de la collaboration et de l'innovation.

« Malgré la numérisation rapide, trop d'entreprises stagnent en matière de cybersécurité. Nous constatons que surtout les plus petits acteurs prennent du retard en raison d'un manque de connaissances et de culture de sécurité, et en raison de la perception erronée qu'ils ne constituent pas une proie intéressante pour les cybercriminels. C'est jouer avec le feu : un piratage ne coûte pas seulement une rançon, il sape le chiffre d'affaires, la continuité et la compétitivité. L'impact est de toute façon bien plus important que les investissements nécessaires. En plus des mesures de base comme les politiques de mots de passe et les pare-feu, nous recommandons aux entreprises de prévoir une analyse des risques, une feuille de route claire et des mesures de détection avancées. La meilleure défense reste une approche en couches. »

Sam Nelen, Partner Risk Advisory
BDO Belgium

DO'S ET DON'TS POUR LES DIRIGEANTS D'ENTREPRISE

DO'S

- Do : planifier des exercices de crise afin que les équipes sachent quoi faire en cas de cyberattaque ou de fuite de données.
- Do : contrôler les mesures de cybersécurité des fournisseurs et des freelances.
- Do : investir dans la sensibilisation des collaborateurs, car le comportement humain est souvent le maillon le plus faible.
- Do : suivre les initiatives européennes comme le Cyber Resilience Act, qui offrent des points de repère et renforcent la confiance.

DON'TS

- Don't : penser qu'en tant que PME vous n'êtes pas une cible. Les hackers savent que les petites entreprises sont souvent moins bien protégées.
- Don't : faire confiance aveuglément à la technologie. Les réflexes humains et le bon sens restent indispensables.