econocom

Les 5 défis en matière de cybersécurité en 2022

“Cela ne m’arrivera pas !”

Saviez-vous que 56% des entreprises réalisent qu’il y a un problème seulement plusieurs mois après une cyberattaque? Ou que 66% des entreprises ont été victimes d’une telle attaque l’année dernière? Un piratage pouvant entraîner des pertes financières et nuire à votre image, c’est donc le genre de choses que l’on préfère éviter. D’autant plus maintenant que l’IT devient plus complexe et que vos données sont plus précieuses que jamais.

La menace en chiffres

Depuis la crise du Corona, la cybercriminalité a augmenté de

600%

Le coût moyen d’une seule cyberattaque est estimé à

3,5

millions d’euros.

Combien de temps une entreprise paie-t-elle les conséquences d’une cyberattaque?

- **67%** la première année
- **22%** la deuxième année
- **11%** la troisième année

Quelle est la cause des cybermenaces?

- **51%** d’attaques criminelles externes
- **25%** de failles système ou de problèmes techniques
- **24%** d’erreurs humaines internes

Quels sont les cinq plus gros défis en matière de cybersécurité?

Ransomware

Il y a de plus en plus de rançongiciels implantés dans le réseau informatique. On parle même maintenant de **double, triple et quadruple extorsion.** Les cybercriminels qui menacent de divulguer vos données sensibles voire même d’avertir vos clients exigent aujourd’hui des sommes quatre fois plus importantes qu’il y a quelques années.

Phishing et spoofing

Indétectables par les logiciels antivirus classiques et une véritable plaie actuellement! La meilleure défense? **Vos propres collaborateurs.**

Professionnalisation des cybercriminels

La professionnalisation galopante d’une **cybercriminalité transnationale organisée** constitue un grand danger, capable de déstabiliser l’économie.

Digitalisation croissante

Les entreprises se digitalisent de plus en plus. Conséquence? Davantage de cibles potentielles pour les cybercriminels, ce qui augmente **les risques** et **l’impact financier** des cyberattaques.

Pénurie de professionnels de la sécurité

Chaque jour sont élaborés des logiciels malveillants toujours plus complexes et avancés. Parallèlement à cela, nous manquons cruellement d’**experts en cybersécurité** pour bloquer ou restaurer les codes corrompus.

Comment la cybersécurité se présente-t-elle en 2022?

La plupart des entreprises sentent que leur cybersécurité actuelle n’est pas à la hauteur des nouveaux défis.

Les entreprises font face à un dilemme unique

- **64%** affirment que l’**IT** est devenu beaucoup **plus complexe** en quelques années
- **44%** déclarent avoir **trop peu de connaissances internes en matière de cybersécurité**
- **55%** reconnaissent que leurs **données revêtent une grande importance** pour l’existence de l’entreprise

Les entreprises ont besoin d’une **approche proactive pour sécuriser leurs données et leur IT.** Les cybercriminels ne sont que trop heureux de pouvoir exploiter la nouvelle réalité informatique complexe et les lacunes de vos connaissances.

Identify

Impossible de protéger vos actifs si vous ne savez pas où ils se trouvent. Votre défense dépendra d’une connaissance claire et complète de tous vos actifs.

- Comment avoir une vue d’ensemble de vos actifs? Est-il possible d’automatiser ce processus?
- Avez-vous une vue d’ensemble de vos données tant dans le cloud qu’en interne et chez les parties externes?
- Avez-vous une connaissance suffisante des actifs gérés ou non-gérés? Savez-vous à quoi ressemble votre structure de données dans son ensemble?
- Quels actifs sont des actifs secondaires et des actifs essentiels?
- Pouvez-vous estimer correctement la valeur de chaque actif?
- Comment mesurer l’efficacité de votre cybersécurité de manière fiable et répétitive?

Protect

L’entreprise dispose d’une cybersécurité en constante évolution, soutenue par tous. Toutes les parties concernées réfléchissent continuellement à l’optimisation du système.

- Les collaborateurs peuvent-ils se connecter en toute sécurité au moyen de l’authentification multifactorielle implémentée?
- Quid de l’hygiène de sécurité du système? La maintenance intermédiaire fait-elle l’objet de suffisamment d’attention?
- Procédez-vous à des tests d’intrusion pour vérifier si vos actifs sont suffisamment protégés?

Detect

L’entreprise mise sur la détection des cybermenaces et veille sur toutes ses équipes.

- La sécurité des actifs est-elle surveillée en permanence?
- Les méthodes utilisées pour le savoir sont-elles suffisamment poussées?
- Les informations obtenues peuvent-elles être interprétées de façon univoque?
- Les activités du SOC sont-elles classées prioritaires en fonction du risque?

Respond

L’entreprise et les collaborateurs savent quoi faire en cas de cybermenace.

- Quel est le plan d’action après une cybermenace? Quelles sont les procédures à suivre lorsque votre cybersécurité est menacée?
- Comment minimiser l’impact d’une cyberattaque?
- Qu’attend-t-on de chaque équipe après une cyberattaque?

Recover

L’entreprise peut continuer à fonctionner même après une cyberattaque et reprendre le cours normal de ses activités très rapidement.

- Quel est le plan d’action à court et à long terme après une cyberattaque?
- Comment s’assurer que les activités de l’entreprise pourront se poursuivre de manière imperturbable, même après une cyberattaque?
- La cyberattaque a-t-elle un impact sur les clients, les partenaires, les parties externes?
- Existe-t-il une sauvegarde des données et des actifs les plus importants?

Être cyber-résilient signifie être totalement **préparé à toutes les formes de cybermenaces** mais aussi disposer d’un **plan d’action efficace** en cas d’imprévu. La cybercriminalité devient de plus en plus inventive. Les entreprises doivent donc évoluer encore plus vite en matière de cybersécurité.

La cyber-résilience consiste à trouver l’équilibre entre **proactivité et réactivité.** Entre action et réaction. C’est pourquoi il s’agit de la meilleure stratégie pour les entreprises qui veulent miser sur une protection complète.

Donnez forme à votre cybersécurité optimale

Econocom constitue votre partenaire en matière de cyber-résilience. Votre meilleure protection commence par un inventaire approfondi de votre dispositif de sécurité. Nous examinons dès lors pour vous:

Votre vue d’ensemble de tous les actifs et les endroits où vous êtes le plus vulnérable aux cybermenaces.

L’efficacité de votre cybersécurité actuelle.

Votre capacité à détecter les menaces et vos connaissances en matière de limitation des dégâts.

La rapidité avec laquelle vous réagissez aux cyberattaques et vous vous rétablissez après celles-ci.

Sur la base de ces informations, nous prodiguons des conseils sur mesure pour votre entreprise. Ensemble, nous élaborons ainsi votre plan d’action solide, totalement indépendant de fournisseurs spécifiques.

En savoir plus sur notre audit de cybersécurité

1. Accueil et installation
2. Collecte de données
3. Rapport final
4. Rapport et conseils

PLUS D’INFOS

econocom IBM