Comment se protéger contre les cyberattaques en entreprise ?

La cybersécurité est un sujet á prendre au sérieux par chaque entreprise. Au vu du nombre record de cyberattaques qui frappent les entreprises de toute taille, une prise de conscience est nécessaire pour mettre en place les ressources nécessaires á une protection efficace

Quelques conseil pour sécuriser le réseau de son entreprise...

Pare-feu

Cela peut paraître banal mais le par-feu est l'un des piliers de la sécurité qui reste l'un des outils les plus importants. Son rôle : bloquer tout accés non autorisé á votre systéme.

Logiciels antivirus

Un antivirus vous avertira en cas d'infection par un virus ou un malware, et beaucoup intégrent des services supplémentaires.
Les antivirus actuels appliquent des mesures de protection utiles, comme la mise en quarantaine des menaces potentielles et leur élimination. Il existe une grande diversité d'antivirus ; vous trouverez facilement celui qui conviendra aux besoins de votre entreprise.

Services d'infrastructure á clé privée

En général, les services d'infrastructure á clé publique (Public Key Infrastructure, PKI) sont uniquement associés aux protocoles SSL ou TLS. Ces technologies de chiffrement des communications serveur que l'on trouve derriére le HTTPS et le cadenas qui s'affiche dans la barre d'adresse de votre navigateur.
Le PKI apporte une réponse á plusieurs problémes de cybersécurité courants et a toute sa place dans la suite de sécurité de chaque organisation.

Le PKI peut être utilisé pour les choses suivantes :

- **Authentification multifacteurs**
- **Création de signatures numériques fiables et conformes.**
- **Chiffrement des communications e-mail et authentification de l'identité de l'expéditeur.**
- **Signature numérique et protection du code.**
- **Identités et confiance dans les écosystémes IoT.**

Test d'intrusion

Les tests d'intrusion sont un excellent moyen de tester les systémes de sécurité de votre entreprise. Lors d'un test d'intrusion, les professionnels de la cybersécurité utilisent les mêmes techniques que les hackers criminels pour détecter les vulnérabilités et points faibles potentiels. Dans ce type de test, on simule le type d'attaque qu'une entreprise pourrait subir : piratage de mots de passe, injection de code ou attaques de phishing.
Une fois le test terminé, les testeurs vous présentent leurs conclusions et peuvent même vous suggérer d'éventuels changements á apporter á votre systéme.

source : www.globalsign.com

...mais ça coûte de l'argent...

Malheureusement, la défense coûte cher. Alors qu'il suffit á un attaquant de trouver et d'exploiter une vulnérabilité, le défenseur doit nécessairement de son côté les traiter toutes. Qui plus est, le nombrede vulnérabilités découvertes chaque année dans les systémes informatiques ne cesse de croître.
Le coût des outils de sécurité reste élevé. Les prix d'un pare-feu ou d'un logiciel antivirus peuvent atteindre 100 000 euros.
Le coût d'une plate-forme de supervision pour gérer ces équipements de sécurité peut se chiffrer á dix fois plus. En outre, leur surveillance doit se faire par des professionnels, or ces compétences manquent sur le marché de l'emploi.
Au total, le déploiement de solutions de protection et de détection se chiffre en millions d'euros chaque année.

source : theconversation.com

Conclusion

Nous avons les connaissances pour contrer un maximum de cyberattaques en entreprise, il existe des solutions trés efficaces.
Mais le souci c'est que cela coûte énormément d'argent.. Les PME peuvent moins se protéger que les trés grandes sociétés comme Google ou autre.

La cybersécurité n'est donc pas accessible pour tous sur un point de vu financier, c'est pour cela que nous avons encore beaucoup de cyberattaques efficaces aujourd'hui..