Cybersecurite : Enjeux, Menaces et Solutions

Auteurs : Costantino Volta, Ruslan Annamammedov, Tuba Demirkiran, Bayarjavkhlan Dugarmaa

Sommaire

Introduction

Nous sommes tous concernes par la cybersecurite car les attaques et les piratages deviennent de plus en plus frequents, même pour les grandes entreprises comme Facebook, Microsoft, ou encore

la police de Shanghai. Une PME doit egalement se proteger, car des tentatives d'intrusion sont constantes. Il est donc essentiel de securiser ses infrastructures numeriques.

Types d'attaques courantes

Deni de service (DDoS)

Une attaque par deni de service consiste a submerger un serveur avec un nombre massif de requêtes pour le rendre indisponible. Exemple : L'État de Vaud a ete victime d'une telle attaque.

Ransomware

Les ransomwares sont des logiciels malveillants qui bloquent l'acces aux donnees d'une entreprise jusqu'au paiement d'une rancon. Ces attaques passent souvent par des pieces jointes infectees dans des e-mails.

Cryptomining

Les pirates exploitent la puissance de calcul des serveurs d'une entreprise pour generer de la cryptomonnaie a leur insu.

Phishing

Le phishing regroupe les techniques visant a obtenir des informations sensibles (comme des mots de passe) via des faux sites web ou des applications frauduleuses comme WhatsApp et Messenger.

Fuites de donnees sensibles

Certaines entreprises, notamment dans le secteur financier, sont souvent la cible de piratages visant a recuperer des informations sensibles sur leurs clients.

Types de dommages

Physiques

Les cyberattaques peuvent cibler des infrastructures critiques, comme les centrales electriques, causant des pannes majeures.

Psychologiques

Les victimes de piratage, notamment en cas de divulgation de dossiers medicaux, peuvent subir un stress intense ou être victimes de chantage.

Atteinte a la reputation

Une cyberattaque peut endommager gravement la reputation d'une entreprise, comme ce fut le cas pour Winbiz, qui a perturbe les operations de milliers de PME.

Perte de confiance

Apres une attaque, les clients perdent souvent confiance dans l'entreprise concernee, nuisant a ses relations commerciales.

Les motivations des cybercriminels

Les cybercriminels agissent pour diverses raisons, mais l'argent est la principale motivation. D'autres motivations incluent l'activisme politique ou social et la cyber-guerre, souvent commanditee par des États pour destabiliser d'autres nations ou entreprises.

Pourquoi les failles de securite persistent-elles ?

Les failles sont souvent dues a des erreurs humaines, techniques ou institutionnelles. L'erreur humaine est a l'origine de 80 % des incidents de cybersecurite. De plus, les lois internationales ne sont pas toujours alignees, ce qui complique la poursuite des cybercriminels operant a l'etranger.

La cybersecurite : un enjeu legal et strategique

La cybersecurite repose sur trois principes fondamentaux :

1. Confidentialite : Proteger les donnees sensibles contre le vol ou l'espionnage.

2. Integrite : S'assurer que les donnees sont exactes et completes.

3. Disponibilite : Garantir que les systemes sont toujours operationnels.

Les entreprises doivent aussi se conformer a des reglementations comme le RGPD (Reglement General sur la Protection des Donnees) en Europe et la nLPD en Suisse. Ces lois visent a proteger les informations personnelles des individus et a garantir que les entreprises traitent ces donnees de maniere responsable.

Les grands principes a respecter pour le traitement des donnees

1. Bonne foi : Ne traiter que les informations reellement necessaires.

2. Proportionnalite : Ne pas collecter plus de donnees que necessaire.

3. Reconnaissabilite : Informer les utilisateurs de la maniere dont leurs donnees sont utilisees.

4. Finalite : Expliquer clairement pourquoi et comment les donnees sont collectees.

Conclusion

La cybersecurite est devenue un enjeu incontournable pour toutes les organisations, grandes ou petites. Elle permet non seulement de se conformer aux lois en vigueur, mais aussi de garantir la confiance des clients et des partenaires. En mettant en place des solutions adaptees, il est possible de minimiser les risques lies aux cyberattaques et de proteger efficacement les donnees sensibles.