
© Axel Abattu

AXEL ABATTU,
EXPERT EN CYBERSÉCURITÉ DE L'ESISAR
LES ENTREPRISES FACE AU RISQUE DE CYBERCRIMINALITÉ

Si vous faites partie de ces 2 petites entreprises sur 5 qui ont déjà essuyé une cyber-attaque (enquête de la CPME en 2019), vous savez que la cybercriminalité n'est pas l'apanage des grands groupes. La menace, déjà présente avant la crise sanitaire, s'est accentuée avec le confinement et l'augmentation des opérations en ligne. Alors quels sont les véritables risques pour les PME ? Comment les évaluer et s'en prémunir ? Autant de questions que nous avons posées à Axel Abattu, expert en cybercriminalité à l'ESISAR et référent auprès de la Région AURA.

On entend souvent parler des attaques vis-à-vis des grands groupes... Les PME sont-elles vraiment concernées par la cybercriminalité ?
Contrairement à ce que l'on pourrait croire, les TPE / PME représentent une cible de choix pour les hackers car leurs systèmes de sécurité sont moins élaborés ; en outre, elles disposent souvent de peu de compétences informatiques en interne. Si des attaques ciblées touchent les grands groupes, les TPE/PME sont davantage visées par les attaques automatisées, diffusées via différents canaux : tentatives de phishing (hameçonnage) par mail, attaques par ransomware (cryptage des données en échange d'une rançon), malwares (logiciels malveillants)...

De quelle manière procèdent les hackers ?
La majorité des cyber-attaques nécessitent un vecteur d'entrée. La plupart du temps, cela passe par la manipulation d'un individu, par mail ou téléphone, pour faire entrer ce programme malveillant dans le système d'information de l'entreprise. L'arnaque au président est fréquente : le pirate se fait passer pour le président de la société afin de faire effectuer un virement sur un compte à l' étranger. De même, les demandes de rançons financières sont plus que jamais d'actualité, comme en témoigne l'exemple récent de l'hôpital de Corbeil-Essonnes.

Quel est le coût d'une cyber-attaque ?
Tout dépend de l'ampleur de l'attaque et de la manière dont elle impacte l'entreprise. Si seuls quelques ordinateurs sont touchés et que l'entreprise peut restaurer les données, les conséquences seront limitées. En revanche, si l'intégralité des serveurs sont bloqués, le coût final risque d'être énorme (enquête technique, remise en service, amélioration des dispositifs de sécurité, perturbation des activités, perte directe de CA, perte de confiance des clients...). Aujourd'hui, plus aucune entreprise ne peut fonctionner sans informatique, que ce soit pour le paiement des salariés, des clients, des fournisseurs...

Comment les entreprises peuvent-elles se prémunir de tels risques ?
La cyber protection, c'est avant tout du bon sens. Les bonnes pratiques sont communiquées par des organismes tels que l'ANSSI* ou le site cybermalveillance.gouv.fr qui mettent à disposition un guide et des fiches pratiques gratuites et personnalisables pour l'entreprise. La protection passe par un ensemble de mesures qui vont de la sensibilisation de l'utilisateur à la mise à jour du matériel. Il faut savoir que l'État aide financièrement les PME à se protéger au travers de différents programmes. Je conseille aussi aux entreprises de se faire auditer par un organisme extérieur pour savoir où se situer par rapport aux risques. Ensuite, il convient d'en tirer les leçons : renouvellement de matériel ou des logiciels, mise à jour du parc informatique, achat d'anti-virus... Idéalement, ce plan d'actions doit se conclure par un audit de conformité pour vérifier le niveau de cyberprotection de l'entreprise.

* ANSSI : Agence Nationale de Sécurité des Systèmes d'Information ■

Comment agir en cas de cyber-attaque ?
En urgence, couper l'intégralité des accès au réseau pour limiter la propagation du virus.
Mobiliser des équipes d'expert pour traiter le problème.
Déposer plainte auprès des services de police ou de gendarmerie – c'est important vis-à-vis des assurances ; pour des questions de responsabilité des dirigeants, et pour obtenir de l'aide.
Contacter les services de l'État susceptibles d'aider l'entreprise ou de dépêcher des experts.
Mettre en place une cellule de crise afin de gérer les différentes problématiques : communication interne / externe, contact éventuel de la CNIL etc.