La cybersécurité

Un nombre de rançongiciels multiplié par 4

Une progression des cyberattaques dans les entreprises

40 %
entreprises ayant subi une cyberattaque ou tentative en France en 2020

4 fois plus d'attaques par rançongiciels entre 2019 et 2020 en France

+ 13 %
de cyberattaques contre les entreprises publiques et privées entre 2020 et 2021

Entretien avec Régis Dubrulle, Délégué régional sécurité numérique à l'ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est l'autorité nationale en matière de sécurité et de défense des systèmes d'information. Cette sécurité des systèmes d'information, ou cybersécurité, est considérée en France comme une priorité nationale. M. Dubrulle livre dans cet entretien quelques-uns des constats d'évolution en la matière.

Le nombre de cyberattaques a été multiplié par 4 entre 2019 et 2020 en France, notamment sous l'effet de la crise du COVID. Quelle est aujourd'hui la tendance nationale ?
La tendance nationale est toujours en augmentation entre 2020 et 2021. Parmi les principales attaques, on retrouve :

- **Les rançongiciels.** Si ces attaques ne sont pas les plus nombreuses, elles provoquent toutefois des conséquences majeures pour les entreprises. L'activité de l'entreprise peut être à l'arrêt pendant une semaine voire 15 jours.
- **Les faux ordres de virement.** Les attaquants se font passer pour des prestataires, des fournisseurs ou des clients et demandent à être payés.
- **Le phishing.** Les attaquants vont tenter de voler les identifiants de messagerie ce qui va permettre de récupérer de la donnée. Ils vont chercher à faire cliquer l'utilisateur sur un lien pour installer un virus ou alors une porte dérobée afin d'installer un CryptoMiner, des logiciels permettant de « *miner* » de la cryptomonnaie.

Les entreprises ligériennes également touchées par les cyberattaques

L'actualité des entreprises ligériennes a été marquée par plusieurs cas de cyberattaques. Quels sont les risques majeurs pour les entreprises et organisations ligériennes ?

Les Pays de la Loire suivent la tendance nationale. **Toutes les entreprises, quelle que soit la taille (TPE, PME, grands groupes) ou le secteur d'activité, sont concernées**. Les organismes de santé et les collectivités locales sont également touchés.
Le premier risque, c'est le rançongiciel. L'entreprise ne peut plus accéder aux applications métiers, ni ouvrir de fichiers. Les entreprises doivent généralement faire appel à une entreprise de remédiation.
Le vol de données est également un risque majeur. Pour pouvoir fonctionner en télétravail avec des outils collaboratifs, beaucoup d'entreprises se sont lancées sur des solutions collaboratives de type Microsoft 365 avec la messagerie dans le Cloud. Cependant, les fonctions de sécurité de ces outils peuvent être paramétrées à un niveau trop bas par rapport à l'ingéniosité des attaquants qui n'ont pas de mal à se connecter à distance sur les messageries des victimes. L'attaquant récupère une quantité importante de données (les adresses e-mail qui se revendent ou les échanges entre professionnels qui peuvent être utilisés pour d'autres types d'arnaques). C'est un risque qu'il faut bien prendre en compte dans les entreprises et ne pas hésiter à renforcer la protection et la sécurité, en mettant en place notamment l'authentification multifacteurs (MFA).

Les entreprises ligériennes sont-elles bien conscientes de ces risques ?

Aujourd'hui, le sujet semble pris en compte par les entreprises ligériennes. Bien qu'on puisse s'en féliciter, les efforts à fournir sont encore nombreux. **Il est nécessaire de sensibiliser les collaborateurs**. C'est un élément clé de la cybersécurité.

Le sujet doit être pris en compte par la Direction des entreprises pour bien définir les risques et les objectifs. **Il est important que les entreprises anticipent, se préparent à une attaque**. Il convient en interne de définir une procédure sur un document préconisant les bons réflexes : quelles sont les premières actions à mener ? Comment gérer la crise ? Comment vais-je communiquer sur cette crise ? Au sein de l'ANSSI nous avons réalisé plusieurs guides : *« Attaques par rançongiciels, tous concernés : comment anticiper, comment réagir ?* » avec des préconisations sur les réactions à adopter, une collection de guides complémentaires dédiée pour s'entraîner, gérer et communiquer avec « *Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique* », « *Anticiper et gérer sa communication de crise cyber* » et « *Organiser un exercice de gestion de crise cyber* ».

L'IA et l'IOT au centre des nouvelles menaces

Quels seront pour vous les risques à anticiper pour les années à venir ? Quelles sont les actions déjà prévues ou à mettre en place ?

Il faut commencer par bien traiter les risques actuels. **Les basiques de la cybersécurité sont importants**. L'ANSSI a ainsi publié deux guides d'hygiène « *La cybersécurité pour les TPE/PME en treize questions* » et un « *Guide d'hygiène informatique* », plus complet, avec 42 mesures.

À l'avenir, **des attaques vont être de plus en plus élaborées à partir de la chaîne de sous-traitance**. Les attaquants voyant que les entreprises durcissent leur système d'information vont s'attaquer à des sous-traitants, espérant rebondir vers des clients et des entreprises plus importantes. L'ANSSI a publié un guide sur l'administration des guides sécurisés expliquant quelles mesures peuvent être prises pour les connexions à distance de la part de sous-traitant. Il importe de « durcir » les accès à distance pour éviter les accès illégitimes. Plusieurs solutions sont possibles : la mise en place de MFA, des accès multifacteurs avec un login, un mot de passe et un deuxième facteur d'identification.

Si on se projette sur le long terme, nous commençons à voir des **attaquants utiliser de l'intelligence artificielle (*IA*), du Machine Learning,** c'est-à-dire de l'autoapprentissage pour mener des attaques d'ingénierie sociale assez avancées notamment avec la deep voice, c'est-à-dire l'imitation par un ordinateur de la voix de quelqu'un afin de lui faire faire des actions. Par exemple, l'attaquant va imiter la voix d'un directeur pour demander à son gestionnaire de faire des opérations malveillantes.

On risque de plus en plus d'attaques sur les objets connectés à internet, notamment **l'IOT industriel**. Les risques liés à la cybersécurité des systèmes d'information industriels sont souvent sous-estimés et trop souvent vulnérables. Pourtant ils sont de plus en plus connectés à internet. La surface d'attaque risque d'augmenter…