Cybersécurité : les 5 points clés du rapport de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a dévoilé son rapport 2018. Un aperçu des menaces cyber analysées en France et en Europe est proposé.

L'espionnage, les jeux d'influence et l'appât du gain sont le moteur des attaquants.

Les cinq grandes tendances mises en exergue par l'ANSSI en témoignent :

1. **Cyber-espionnage** > il constitue le risque le plus élevé pour les organisations.

« Des groupes très organisés préparent ce qui ressemble aux conflits de demain », a déclaré Guillaume Poupard, directeur général de l'ANSSI. Leur objectif : s'introduire dans les infrastructures systèmes « les plus critiques » et exfiltrer des données stratégiques.

Défense, santé, recherche… Des secteurs d'activité d'importance vitale sont ciblés par des groupes d'attaquants disposant d'importants moyens financiers pour planifier, discrétement, des attaques techniquement sophistiquées et ciblées, selon l'Agence.

2. **Attaques indirectes** > Les attaques informatiques ciblant les fournisseurs et les prestataires techniques de grands groupes sont en hausse.

« Les attaquants exploitent de plus en plus les relations de confiance établies entre partenaires pour accéder aux informations qu'ils convoitent », a ajouté l'ingénieur.

La compromission d'un seul intermédiaire permettant parfois aux attaquants ou à leurs commanditaires d'accéder aux réseaux de plusieurs organisations.

3. **Déstablilisation** et jeux d'influence > ces opérations ont un degré modére de technicité, selon l'ANSSI. Les cibles sont choisies pour leur « apparente » vulnérabilité.

Ces attaques (de l'attaque par déni de service au sabotage) « ont été particulièrement nombreuses en 2018 ». Elle peuvent avoir été revendiquées « depuis la France ou l'étranger par des individus isolés comme par des groupes d'attaquants », a précisé dans son rapport l'autorité nationale de défense et de sécurité des systèmes d'information.

4. **Cryptojacking** > des attaques multiples destinées à enrichir les attaquants.

L'ANSSI dit avoir observé « tout au long de l'année une multiplicité d'attaques » visant à compromettre un grand nombre d'équipements pour y déposer des mineurs de cryptomonnaies. Les attaquants peuvent alors « se servir de la puissance de calcul cumulée de ces systèmes » pour valider de nouvelles transactions.

5. **Fraude en ligne** > un classique toujours très en vogue sur Internet.

La fraude et les campagnes d'hameçonnage (phishing) observées en 2018 ont surtout visé « des cibles moins exposées mais plus vulnérables » que de grands groupes. Ce fut le cas notamment de

collectivités territoriales et d'acteurs du secteur de la santé.

Ces campagnes ont différents objectifs, dont le vol de données personnelles, le versement d'une rançon après blocage d'un système par ransomware ou le chiffrement de fichiers, le minage de cryptomonnaies ou encore la constitution de réseaux zombies (botnets).

Enfin, si les migrations vers le cloud peuvent présenter un risque, elles offrent également d'importantes opportunités pour un grand nombre d'acteurs.

Partenariats

Selon Guillaume Poupard, « la 'bonne nouvelle' dans tout ça, c'est qu'il devient de plus en plus difficile pour les décideurs d'ignorer cette menace. »

Pour l'affronter et conforter ses missions d'expertise auprès d'administrations et d'entreprises, opérateurs de services essentiels (OSE) de la directive NIS inclus, l'ANSSI ambitionne de renforcer ses partenariats publics (DINSIC en tête) et privés.

Un écosystème que l'ANSSI souhaite vertueux. Pour le pilote du service à compétence nationale, « progressivement, on assiste au sein des organisations à un rapprochement entre sécurité numérique et préoccupations économiques, politiques et sociétales. »

(crédit photo © Shutterstock)