Pourquoi l'email est le premier vecteur de cybercriminalité dans le monde

L'email n'est pas mort, bien au contraire. C'est même aujourd'hui le principal canal de communication numérique dans le monde, avec quatre milliards d'usagers qui font transiter plus de 300 milliards de courriers électroniques chaque jour, dont près de la moitié dans le cadre professionnel.

Son histoire commence dans les années 1960 avec ARPANET, l'ancêtre d'Internet appartenant à l'époque au ministère américain de la défense. Mais c'est en 1971 que l'ingénieur américain Ray Tomlinson a imaginé une forme de communication plus directe en envoyant des messages d'un ordinateur à un autre, utilisant le caractère @ comme séparateur… L'email était né.

Un temps utilisé dans les universités et les administrations publiques, ainsi que pour les communications en entreprise, l'email est réellement devenu populaire dans les années 90, avec le lancement du premier service gratuit basé sur le web (HTML).

Epidémie de virus informatiques

Mais c'est aussi à cette époque que les premières dérives d'Internet commencent. A mesure qu'il se développe et devient de plus en plus rapide, l'utilisation massive de l'email en fait un excellent vecteur de propagation : la tentation est trop grande pour des acteurs malveillants de diffuser des virus informatiques le plus largement et le plus rapidement possible par ce canal.

Le premier virus à se propager en masse par email était le ver Ska, alias Happy99, en janvier 1999. Profitant de la standardisation de Microsoft Outlook, il est passé d'ordinateurs en ordinateurs sous forme de pièce jointe, qui si elle était exécutée, ouvrait une fenêtre affichant un feu d'artifice animé. Puis ont suivi beaucoup de logiciels malveillants, comptant parmi eux les plus destructeurs de l'histoire : Melissa, ILOVEYOU… puis les célèbres Wannacry et NotPetya.

Il est devenu difficile d'ignorer les trop nombreuses campagnes de rançongiciels destructeurs et autres attaques ciblées par email. Presque toutes ces cyberattaques ont deux choses en commun : elles n'épargnent personne, et ont besoin de l'humain pour fonctionner. 94 % des cyberattaques sont aujourd'hui initiées via la boîte email et 99 % d'entre elles nécessitent une action humaine pour se déclencher (clic, ouverture de pièce-jointe). On comprend alors aisément l'importance de l'ingénierie sociale, ce véritable piratage psychologique qui entraîne les destinataires à cliquer…

Objectif : protéger l'email

L'email n'étant pas près de disparaître, mieux vaut mettre tous les moyens en œuvre pour protéger ce canal et contourner les assauts de cybercriminels plus motivés et professionnalisés que jamais pour gagner de l'argent sur le dos des utilisateurs et des entreprises. Heureusement, de nombreuses initiatives à travers le monde ont été lancées pour contrer ces menaces et tenter de sécuriser « plus nativement » l'infrastructure email.

Parmi les initiatives les plus emblématiques, on peut saluer la mise en œuvre du standard DMARC (Domain-based Message Authentication, Reporting & Conformance).

Créé en 2012 par des opérateurs majeurs de messagerie tels que Google, Yahoo!, AOL et Microsoft, DMARC constitue sans doute à ce jour l'arme la plus puissante pour lutter contre le spoofing (usurpation d'identité d'une marque de confiance) et le phishing (hameçonnage) grâce à une authentifier des expéditeurs.

D'autres initiatives continuent en parallèle de se développer, comme le chiffrement TLS (Transport Layer Security) ou les extensions de sécurité du DNS (Domain Name System) pour protéger toutes les interactions de type page web consultée, email envoyé ou photo récupérée sur un réseau social. Ces outils sont amenés à être utilisés de plus en plus systématiquement dans les prochaines années pour sécuriser notre monde numérique.

In fine, l'humain étant dans l'œil du cyclone, c'est aussi et surtout dans cette direction qu'il faut travailler pour se protéger. Les entreprises ne peuvent désormais plus s'affranchir d'une réelle stratégie de cybersécurité centrée sur les personnes, incluant des programmes de sensibilisation et de formation réguliers et approfondis.

Vers une nouvelle pandémie mondiale ? A l'image de l'affaire SolarWinds, de nouvelles formes d'attaques beaucoup plus sophistiquées font désormais leur apparition dans le paysage de la cybermenace.

Avec elles, c'est toute la confiance numérique qui est mise à mal et l'extrême dépendance des organisations publiques et privées auprès de certains acteurs ne peut qu'être source d'inquiétudes, notamment vis à vis des risques d'espionnage ou de cataclysme numérique systémique.

Si un opérateur de ressources numériques d'envergure mondiale tel que Microsoft perd le contrôle, alors cette pandémie numérique presque annoncée impliquera tout notre ensemble d'outils de collaboration… Et une telle perspective risque vite de devenir incontrôlable.