Communiqué de presse

swisscom

Cybercriminalité: d'où vient le danger?

Le dernier Cyber Security Threat Radar de Swisscom montre comment les cybercriminels se sont adaptés à la pandémie: avec des attaques contre le télétravail et l'utilisation des dernières technologies IA.

Le flot des cybermenaces ne faiblit pas. Les grandes sociétés et les PME continuent d'être dans le viseur des hackers. Le basculement de nombreux collaborateurs en télétravail, lié à la pandémie, a fourni aux cybercriminels une nouvelle cible bienvenue. Ces derniers ont donc adapté leurs méthodes d'attaque à la nouvelle situation.

Le dernier Cyber Security Threat Radar le montre: le nombre d'attaques reste à un niveau élevé. Si les méthodes d'attaque individuelles – plutôt classiques – sont en déclin, les approches intelligentes et en général basées sur l'IA se multiplient. Les entreprises et les organisations sont donc appelées à redoubler de vigilance – les méthodes des attaquants évoluent en permanence.

Nouvelles exigences, nouvelles méthodes d'attaque

Aujourd'hui, l'hétérogénéité des lieux de travail constitue par exemple l'un des plus grands défis en matière de sécurité IT. Le déploiement immédiat du télétravail a été l'une des choses les plus compliquées que les services IT et de sécurité ont eu à gérer dans un passé récent. Le home office tout comme les modèles de travail mobiles et agiles, tels que «Bring your own device», offrent de grandes possibilités – mais ils constituent aussi de nouvelles cibles. Des cibles que les hackers savent exploiter avec habileté.

Les attaques ayant recours à l'intelligence artificielle, dites AI-based Attacks, sont elles aussi de plus en plus courantes et sont répertoriées parmi les menaces croissantes dans le Cyber Security Threat Radar. Elles sont par exemple utilisées pour la désinformation ciblée, comme dans le cas des deepfakes. La chaîne TikTok «Deeptomcruise» a récemment fait sensation. Des vidéos montraient Tom Cruise faire des tours de magie et jouer au golf. Mais le véritable tour de magie était la vidéo elle-même: car une fois n'est pas coutume, la star hollywoodienne n'était pas devant la caméra, il n'était même pas au courant. Il s'agissait d'un fake quasi parfait, créé avec l'intelligence artificielle.

Grâce à elle, les cybercriminels sont en mesure d'exploiter toute une série d'informations pour créer automatiquement un profil artificiel très difficile à identifier comme faux. Le rapport présente les mesures que les entreprises peuvent initier pour se protéger contre ce type de situations et bien d'autres encore.

La boussole dans le cybermonde

Avec le Cyber Security Threat Radar, les spécialistes Swisscom disposent d'un outil pour déterminer le niveau de menace actuel en Suisse. Le rapport explique les motivations des cybercriminels et dévoile leur façon de procéder. Il examine et observe les tendances et les défis, les évalue et rassemble toutes les connaissances des experts pour offrir une vue d'ensemble du niveau de menace et de son évolution en Suisse. En outre, il indique des mesures préventives particulièrement efficaces pour détecter au mieux et au plus tôt une attaque. Le Cyber Security Threat Radar sert de guide et de boussole pour évoluer en toute sécurité dans le cybermonde.

Berne, le 16 avril 2021

Informations complémentaires:

www.swisscom.ch/security