**Philippe Vuilleumier**
Chief Security Officer, Swisscom

# Leichtes Spiel für Hacker

Täglich berichten Medien von neuen Cyberattacken auf Unternehmen und Organisationen. Cyberkriminelle dringen in fremde IT-Infrastrukturen ein, verschlüsseln Daten, blockieren Systemzugänge und fordern Lösegeld für den Entschlüsselungscode. Von diesen sogenannten Ransomware-Attacken sind auch Regierungen nicht gefeit. Mitte Mai musste Costa Rica nach einem Cyberangriff den nationalen Notstand ausrufen.

Die Angreifer haben oft leichtes Spiel: Sie stossen auf ungepatchte Systeme, VPN-Zugänge ohne Multi-Faktor-Authentifizierung oder eine IT, die die Installation von Malware nicht verhindert. Und das Geschäft mit gestohlenen Daten ist für die Cyberkriminellen äusserst lukrativ.

Dass die Flut an Cyberbedrohungen ungebrochen hoch ist, zeigt auch der Cyber Security Threat Radar von Swisscom. Der Report gibt eine Übersicht zu den aktuellen Bedrohungen in der Schweiz. Er deckt das Vorgehen der Cyberkriminellen auf und erklärt, in welche Angriffsmethoden sie ihre Energie stecken. Waren bisher vor allem Grosskonzerne und Betreiber kritischer Infrastrukturen wie Energieversorger und Spitäler im Visier, so trifft es inzwischen vermehrt KMU und auch Gemeinden.

Die gute Nachricht: Niemand ist den Cyberkriminellen schutzlos ausgeliefert. Mit den richtigen Massnahmen lässt sich das Risiko, Opfer zu werden, massiv verringern. Und die ersten Schritte zu einer sicheren IT-Umgebung können mit einfachen Fragen beginnen wie: Verwende ich ein sicheres Passwort? Benutze ich Multifaktorauthorisierung? Habe ich die Software-Updates gemacht? Gibt es regelmässige Back-ups? Auch offline? Eine gute Einschätzung erhält man auch über den IKT-Minimalstandard, ein kostenloses Assessment-Tool des Bundesamts für wirtschaftliche Landesversorgung BWL.

Die besten technischen Sicherheitsvorkehrungen alleine garantieren aber noch keinen Schutz, denn 90% aller erfolgreichen Cyberattacken geht menschliches Fehlverhalten voraus. Deshalb sind im Kampf gegen Cyberkriminelle die Mitarbeitenden die wirksamste Waffe. Sie sind das wichtigste Glied in der Verteidigungskette und sollten regelmässig auf Cyberrisiken sensibilisiert werden.

# Un jeu d'enfant pour les pirates

**Chaque jour, les médias font part de nouvelles cyberattaques contre des entreprises et des organisations. Les cybercriminels s'introduisent dans les infrastructures informatiques de tiers, cryptent les données, bloquent l'accès aux systèmes et exigent une rançon pour la clé de décryptage. Même les gouvernements ne sont pas à l'abri de ces attaques par ransomware : mi-mai, le Costa Rica a dû déclarer l'état d'urgence national après une cyberattaque.**

**Les hackers ont souvent la partie facile : ils tombent sur des systèmes non patchés, des accès VPN sans authentification multi-facteurs ou une informatique qui n'empêche pas l'installation de logiciels malveillants. Et le commerce des données volées est extrêmement lucratif pour les cybercriminels.**

**Le Cyber Security Threat Radar de Swisscom montre, lui aussi, que le flot de cybermenaces est toujours aussi important. Ce rapport donne un aperçu des menaces actuelles en Suisse. Il révèle les procédés utilisés par les cybercriminels et explique dans quelles méthodes d'attaque ils investissent leur énergie. Si jusqu'à présent, ils visaient principalement les grands groupes et les exploitants d'infrastructures critiques tels que les fournisseurs d'énergie et les hôpitaux, les PME et même les communes sont désormais de plus en plus touchées.**

**La bonne nouvelle est que personne n'est sans défense face aux cybercriminels. En prenant les bonnes mesures, il est possible de réduire considérablement le risque d'être victime d'une attaque. Et les premiers pas vers un environnement informatique sécurisé peuvent être de se poser de simples questions : est-ce que mon mot de passe est sûr ? Est-ce que j'utilise une autorisation à facteurs multiples ? Est-ce que j'ai réalisé la mise à jour des logiciels ? Est-ce que des sauvegardes sont effectuées régulièrement ? Et ce, également hors ligne ? Il est aussi possible d'obtenir une bonne évaluation de sa situation grâce à la norme minimale pour les TIC, un outil d'évaluation gratuit de l'Office fédéral pour l'approvisionnement économique du pays (OFAE).**

**Les meilleures mesures de sécurité techniques ne garantissent toutefois pas à elles seules une protection, car 90% des cyberattaques couronnées de succès découlent d'une erreur humaine. C'est pourquoi, dans la lutte contre les cybercriminels, les collaborateurs constituent l'arme la plus efficace. Ils sont le maillon le plus important de la chaîne de défense et devraient être régulièrement sensibilisés aux cyber-risques.**