



Cyberkriminalität: Woher die Gefahr droht

Der aktuelle Cyber Security Threat Radar von Swisscom zeigt, wie Cyberkriminelle infolge der Pandemie ihre Angriffsmethoden angepasst haben: mit Attacken aufs Homeoffice und mit Einsatz neuester KI-Technologie.

Die Flut an Cyberbedrohungen ist ungebrochen hoch. Grosse Firmen und KMU stehen nach wie vor im Visier von Hackern. Der pandemiebedingte Wechsel vieler Angestellten ins Homeoffice bot den Cyberkriminellen ein willkommenes neues Angriffsziel. Entsprechend haben sie ihre Angriffsmethoden den neuen Gegebenheiten angepasst.

Der neuste Cyber Security Threat Radar zeigt: Die Anzahl Angriffe bewegt sich nach wie vor auf konstant hohem Niveau. Während einzelne – eher klassische – Angriffsmethoden rückläufig sind, kommen intelligente und oftmals KI-gesteuerte Vorgehensweisen vermehrt zum Einsatz. Unternehmen und Organisationen werden dadurch zusätzlich gefordert den Überblick zu behalten – die Methoden der Angreifer entwickeln sich stetig weiter.

Neue Voraussetzungen, neue Angriffsmethoden

So zählt etwa Workplace Heterogeneity inzwischen zu den grössten Herausforderungen in der IT-Sicherheit. Die sofortige Entsendung ins Homeoffice war eine der grössten Herausforderungen, die IT- und Sicherheitsabteilungen in jüngster Vergangenheit bewältigen mussten. Homeoffice sowie mobile und agile Arbeitsmodelle, wie beispielsweise "Bring your own device", bieten grosse Chancen – sie eröffnen aber auch neue Angriffsflächen. Und diese Entwicklung nutzen Angreifer gekonnt zu ihrem Vorteil aus.

Auch Angriffe mittels Einsatzes künstlicher Intelligenz, sogenannte AI-based Attacks, treten vermehrt in den Vordergrund und werden im Cyber Security Threat Radar als eine zunehmende Bedrohung eingestuft. Sie kommen beispielsweise bei gezielter Desinformation zum Einsatz, wie man sie etwa von Deepfakes kennt. So sorgte jüngst der Tiktok-Kanal «Deeptomcruise» für Furore. Auf Videos zeigte Tom Cruise Zaubertricks und spielte Golf. Der eigentliche Zaubertrick war aber das Video selbst: Denn dafür ist der Hollywoodstar für einmal nicht vor der Kamera gestanden, er wusste nicht mal davon. Es handelt sich um eine fast perfekte Fälschung, die dank künstlicher



Intelligenz geschaffen worden ist. Durch sie sind Cyberkriminelle in der Lage, aus unterschiedlichsten Informationen automatisiert ein künstliches Profil zu erschaffen, das nur sehr schwer als Fälschung erkennbar ist. Welche Gegenmassnahmen Unternehmen gegen diese und andere Herausforderungen treffen können, wird im Report erläutert.

Kompass in der Cyberwelt

Mit dem Cyber Security Threat Radar haben die Spezialistinnen und Spezialisten von Swisscom die aktuelle Bedrohungslage in der Schweiz ermittelt. Der Report erklärt die Motivation der Cyberkriminellen und deckt ihr Vorgehen auf. Er betrachtet und beobachtet Trends und Herausforderungen, bewertet diese und verschafft durch das Bündeln von Expertenwissen einen Überblick zur Bedrohungslage und deren Entwicklung in der Schweiz. Zudem zeigt er, welche Gegenmassnahmen besonders effektiv sind, um Angriffe bestmöglich und frühzeitig zu erkennen. Der Cyber Security Threat Radar dient als Leitfaden und Kompass, um sicher durch die Cyberwelt zu manövrieren.

Bern, 16. April 2021

Weiterführende Informationen:

www.swisscom.ch/security