Vor wem sollten sich Unternehmen schützen? Wer sind die Angreifer?

Ohne Internet geht heute gar nichts mehr. Weder am Arbeitsplatz noch in der Freizeit. Aber das Cybernet ist voller Gefahren. Wer die Gefahren kennt, hat bessere Chance, Sie erfolgreich zu vermeiden.

Warum wird das Cybernet immer gefährlicher?

- Das Cyberverbrechen ist erwachsen geworden. Es ist heute nicht mehr Freizeitvergnügen von jugendlichen Computer-Nerds, sondern „Big Business".
- Hinter den externen Bedrohungen steckt mehr organisierte Kriminalität. Online-Verbrecherbanden lassen sich zum Beispiel von erfahrenen Programmierern Schadsoftware entwickeln. Damit stehlen sie Geld oder persönliche Daten. Kriminelle bieten nicht nur gestohlene Daten zum Kauf an, sondern auch gleich noch Programme, mit denen sich vertrauliche Informationen ausspionieren lassen

Wussten sie zum Beispiel, dass:

- vor zehn Jahren Viren und andere Formen von Malware hauptsächlich von jungen Amateurprogrammierern geschrieben wurden, die damit einfach nur auf sich aufmerksam machen wollten?
- laut einem Report von Verizon 70 Prozent aller untersuchten Fälle von Datenmissbrauch von Externen ausgingen, 48 Prozent auf ‚Insider' zurückzuführen waren?
- laut World Economic Forum allein im Jahr 2009 im Internet Diebstahl im Wert von einer Billiarde (1 Million Millionen) US-Dollar begangen wurde?

AVG

Wer sind die Angreifer?

Hacker

Hacker sind per Definition keine bösen Menschen, sondern sie beschäftigen sich nur intensiv mit Computern und deren Sicherheit. Ihr Ziel war es stets, möglichst elegant Schwachstellen aufzudecken und die Lücken in sicher geglaubten Systemen zu entlarven, um Hersteller und Regierungen zu einem sicheren Umgang zu bewegen. In einigen Fällen verschaffen sich Hacker illegalen Zugang zu Systemen, um deren Schwächen aufzudecken, nicht jedoch um zu stehlen oder Schaden anzurichten (Hacker-Ethik).

Cracker

Nach den Hackern kamen die Cracker. Sie wollen ganz bewusst in ein System eindringen und Schaden anrichten. Dazu brauchten Sie – ebenso wie die Hacker – ein enormes Wissen. Teilweise gab und gibt es unter Hackern und Crackern auch regelrechte Wettläufe um die Ehre, als erster ein bestimmtes System überwunden zu haben.

Script Kiddies

Die Werkzeuge der Hacker und Cracker haben sich so weit einwickelt, dass sie auch ein weitgehend ahnungsloser Schüler anwenden kann. Häufig ist der Ablauf zur Erzeugung von Schaden in diesen Werkzeugen weitgehend ablaufgesteuert – wie in einem Skript. Daher trägt diese Gruppe den Namen ‚Skript Kiddies'. Sie sind oft unreif und können das Ausmaß ihrer Handlungen nicht absehen. Sie wollen Aufsehen erregen und Anerkennung gewinnen.

Cyber-Kriminelle

Cyber-Kriminelle nutzen das Internet, um gezielt Verbrechen zu begehen. Die Tatbestände reichen von Betrug über Diebstahl bis hin zu Nötigung und Erpressung. Die Cyber-Kriminellen nutzen dazu häufig Software, die Sie auf den PCs ihrer Opfer einschleusen oder manipulierte Webseiten, meist jedoch beides. Sie haben es auf Kreditkarten-Informationen oder Bankdaten abgesehen, sie ergaunern Passwörter und ganze Identitäten. Hinter den Cyber-Kriminellen steckt eine regelrechte Industrie von Lieferanten, die Schadsoftware in scheinbar nützlichen Programmen, Musik-, Video oder Bilder-Downloads verstecken oder die illegal kopierte Inhalte zum Kauf anbieten.

Die erschreckende Entwicklung der jüngsten Zeit: Die Kriminellen brauchen in letzter Zeit immer weniger technisches Know-how, denn sie bekommen für wenige hindert Euro bereits sehr leistungsfähige, fertige Einbruchswerkzeuge auf dem Schwarzmarkt, die auch ein gewöhnlicher Laie bedienen kann. Das verstärkt die Bedrohung stetig weiter. De facto sind viele Cyber-Kriminelle vom technischen Know-how her Skript Kiddies mit zum Teil schwerst kriminellen Motivationen.

Cyber-Spione

Wissen ist Macht und Geld. Cyber-Spione haben das Ziel, in Forschungslabors, Entwicklungsabteilungen, Regierungsstellen einzudringen und die dort hinterlegten Informationen zu stehlen. Gerade der Mittelstand ist immer häufiger Ziel solcher Attacken, etwa wenn Mitbewerber oder konkurrierende Nationen Pläne oder Angebotsunterlagen entwenden.

Cyber-Aktivisten, Cyber-Terroristen

Diese Gruppe verfolgt ideologische Ziele – etwa indem Sie Webseiten mit politischen Botschaften verunstaltet oder versucht, wesentliche Infrastrukturen lahm zu legen. Auch immer mehr Nationalstaaten betreiben intensive Forschungen, um auf diese Weise kriegerische Handlungen zu verhindern oder auch auszuführen.

Ihr Fachhändler:

AVG