Hacking: Infos und Tipps für Unternehmen

Wie man sich vor Hackerattacken schützt

Der Begriff Hacker beschreibt ursprünglich Tüftler und Bastler. Menschen, die versuchen, durch Improvisation und viel Querdenken neue Lösungen zu finden. Die Zweckentfremdung einer Geschirrspülmaschine zum Kochen von Fisch ist zum Beispiel so ein Hack. Und genau solche Typen von Entwicklern waren am Anfang des Computerzeitalters enorm wichtig. Die Möglichkeiten dieser Rechner waren sehr begrenzt und die Hacker haben dem damaligen Blechtrottel mit viel Kreativität zu immer neuen Anwendungen verholfen. Heute versteht die Öffentlichkeit unter einem Hacker einen talentierten Programmierer, der mit bösartiger Software anderen schadet, das entspricht aber nicht ganz dem realen Spektrum.

Böse Hacker

Medial haben sie sicher die meiste Aufmerksamkeit. Kriminelle Computerexperten, die ihr Wissen nutzen, um Schadsoftware in Umlauf zu bringen. Damit sammeln sie z.B. Kreditkartendaten, die sie dann verkaufen, oder sie schaffen sich Zugriff auf ein fremdes Online-Shop-Konto. Auch Erpressung kommt vor, indem wichtige Dateien auf dem Computer gesperrt oder gelöscht werden oder die Veröffentlichung sensibler Informationen angedroht wird. Ihre Welt ist das Darknet, ein Teil des Internets, wovon Otto Normalverbraucher meist nichts mitbekommt. Mit spezieller Software, die die Herkunft der Nutzer verschleiert, kann man sich dort bewegen. Im Darknet findet reger Erfahrungsaustausch unter Gleichgesinnten statt, Code für Schadsoftware ist hier zu finden, es ist der Marktplatz für die erbeuteten Daten und vieles mehr. In Österreich geht man von ca. 5000 zielgerichteten Hacker-Attacken pro Tag aus.

Schutz vor Hacking-Angriffen

Seriöse Statistiken sprechen davon, dass jedes vierte Unternehmen in Mitteleuropa einmal pro Jahr Angriffsziel wird. Im Bereich der Finanzdienstleister sogar jedes zweite. Hackerattacken haben im letzten Jahrzehnt im 1.000 % zugenommen. Doch nicht jede Attacke ist von Erfolg gekrönt. Selbst KMU können sich mit relativ einfachen und kostengünstigen Mitteln schützen: ein aktueller Virenschutz auf jedem Gerät erkennt z.B. verseuchte Email-Anhänge. Diese sind ein beliebter Trick, um das System mit Schadsoftware zu infizieren, die den Hackern dann den Zutritt ermöglicht. Eine richtig eingestellte Firewall erkennt verdächtige Zugriffe. Und gut geschulte Mitarbeiter erkennen oft schon im Ansatz, wenn das Unternehmen möglicherweise gerade Angriffsziel wird. Generell gehen Hacker den Weg des geringsten Widerstands. Ein paar (übrigens auch gesetzlich vorgeschriebene) Schutzmaßnahmen machen ihnen das Leben bereit so schwer, dass sie es gemäß dem alten Florianiprinzip üblicherweise beim Nachbarn probieren.

Gute Hacker

Wie schützt man sich gegen Programmierer, die nichts Gutes im Sinn haben? Mit ebenso talentierten Codeschreibern, die sich aber an die Grenzen der Gesetze halten. Auch sie nennen sich oft selbst Hacker und werden z.B. von Unternehmen beauftragt, die Sicherheit der IT-Systeme zu testen, indem sie Angriffe simulieren. Google veranstaltet unter anderem regelmäßig Hackathons, bei denen Programmierer weltweit aufgefordert werden, Sicherheitsbarrieren zu knacken. Wer es schafft bekommt ein Preisgeld und Google erhält dafür einen "Stresstest" der eigenen Software. Ein weiteres Betätigungsfeld entspricht der Ursprungsdefinition. Diese Hacker entwickeln oft Software, die die technischen Möglichkeiten auf neue Art und Weise nutzt oder Beschränkungen - im Bereich des Legalen - umgeht. Facebook hat z.B. lange gebraucht, um die eigene App auf das iPad zu bringen. Nach der Anstellung eines bekannten Hackers von Apple-Geräten dauerte die Veröffentlichung nicht mehr allzu lange.

Die Grauzone

Natürlich gibt es nicht nur böse und gute Hacker. Die Grenzen verschwimmen, sind eigentlich nicht zu ziehen und viele Hacker halten sich ständig in einer Grauzone auf. Ihr Ziel ist es nicht, sich durch schadhaften Code zu bereichern. Sie haben höhere Ziele und eine ganz eigene Ethik. Aufdecker von Sicherheitslücken kommen oft aus diesem Bereich. Dehr gefragt sind ihre Künste auch, wenn es darum geht, eigentlich zugeknöpfte Geräte wie z.B. das iPhone zu öffnen, damit man sie umfangreicher und individueller nutzen kann. Geldinteressen stecken hier nicht dahinter, legal sind ihre Aktivitäten deshalb natürlich trotzdem nicht.

Videos zum Thema

- E-Day:16 - Die Geschäftsmodelle der Hacker, Alexander Mitter, Nimbusec GmbH
- E-Day:16 - Erpressung und Trickbetrug im Internet, Peter Kieseberg, SBA Research
- E-Day:16 - Die Guten, die Bösen und die Ahnungslosen, Marion Marschalek, G DATA Advanced Analytics
- E-Day:16 - Aktuelle Entwicklungen im Bereich Cybercrime, Gert Seidl, Cybercrime Competence Center, Bundeskriminalamtes

Stand: 18.12.2018