Unseriöse Schlüsseldienste >
< Betrügerische Spendensammler

Cybercrime – Angriffe auf Unternehmen

Internet-Kriminalität schädigt die Wirtschaft

Von Cybercrime sind große Konzerne genauso wie kleine Betriebe betroffen

Gehackte Unternehmensnetzwerke und Diebstahl sensibler Daten von Firmen-Computern: Cybercrime ist zur allgegenwärtigen Gefahr für Großkonzerne wie auch für mittelständische Betriebe geworden. Der wirtschaftliche Schaden bundesweit beträgt einige Milliarden Euro jährlich.

Cyberangriffe auf Unternehmen in Deutschland

„Die globalen Kosten von Cybercrime“ lautet der Titel einer Studie, die das Center for Strategic and International Studies zusammen mit dem IT-Security-Anbieter McAfee im Juni 2014 veröffentlichte. Die Erhebung belegt, dass die finanziellen Schäden durch Cybercrime gemessen am Bruttoinlandsprodukt (BIP) nirgendwo so hoch sind wie in Deutschland: Hier sollen sie bei 1,6 Prozent des BIP liegen. Zum Vergleich: In den USA und Norwegen beträgt der Wert nur 0,64 Prozent, in China 0,63 Prozent. In der EU werden laut der Studie pro Jahr rund 150.000 Arbeitsstellen durch Verbrechen im Zusammenhang mit Datenverarbeitung vernichtet. Cybercrime ist ein globales Phänomen, das lokal großen Schaden anrichtet. Die IHK Hannover hat im Juli 2014 die Ergebnisse einer Befragung zu Cybercrime vorgestellt. Demnach ist schon jedes dritte Unternehmen in Norddeutschland Opfer von Cyberattacken geworden. Dabei hatten weder Branchenzugehörigkeit, noch Unternehmensgröße oder das IT-Nutzungsverhalten einen wesentlichen Einfluss auf die Angriffswahrscheinlichkeit. Die Umfrage macht auch deutlich, dass das Anzeigeverhalten der Unternehmen bei Cybercrime sehr zurückhaltend ist.

Wer ist gefährdet?

„Gefährdungen entstehen immer dort, wo Werte vorhanden sind. Gerade in Deutschland gelten sehr viele kleine und mittelständische Unternehmen (KMU) als besonders innovativ“, so Tim Griese, Pressereferent des Bundesamts für Sicherheit in der Informationstechnik (BSI). Diese Unternehmen verfügten über umfangreiches, spezialisiertes Know-How. Viele unter ihnen seien „Hidden Champions“, so Griese. Zahlreiche Firmen verfügen über Patente und wichtiges geistiges Eigentum. „Das weckt ebenso Begehrlichkeiten wie Informationen zu Vorstandsentscheidungen eines Großkonzerns.“

Cybercrime-Straftatbestände:

- Ausspähen von Daten
- Abfangen von Daten
- Veränderung von Daten
- Fälschung beweiserheblicher Daten
- Computerbetrug
- Computersabotage

Anzeichen für einen Hack

Oft merken Unternehmen gar nicht, dass sie Opfer eines Cybercrime-Angriffs geworden sind. Folgende Anzeichen können darauf hinweisen, dass sich online ein Außenstehender widerrechtlich im Firmensystem befindet:

- Ein unbekannter Nutzer ist im System eingeloggt.
- Es laufen seltsame Prozesse auf dem System, die viele Systemressourcen benötigen.
- Die Rechner sind von einem Schadprogramm
- Jemand versucht von außerhalb, etwa durch Portscanning, in das System einzudringen.
- In kurzer Zeit erreichen viele Datenpakete das System.

Wie können sich Unternehmen schützen?

Die Anzeichen für einen Cyberangriff können sehr unterschiedlich sein

Als ganzheitliches Konzept für Informationssicherheit hat sich das Vorgehen nach den IT-Grundschutz-Katalogen des Bundesamts für Sicherheit in der Informationstechnik als Standard etabliert. Der IT-Grundschutz hilft beim Aufbau einer Sicherheitsorganisation. Zugleich bietet er eine umfassende Basis für die Risikobewertung, die Überprüfung des vorhandenen Sicherheitsniveaus und die Implementierung der angemessenen Informationssicherheit. Dieses Vorgehen empfiehlt das BSI ab einer Unternehmensgröße von etwa 30 Mitarbeitern. Informationen zu Schutzmaßnahmen speziell für kleine und mittelständische Unternehmen bietet die Webseite der [externer Link] Allianz für Cybersicherheit, www.allianz-fuer-cybersicherheit.de [/externer Link] die das BSI gemeinsam mit dem Branchenverband BITKOM initiiert hat. Hier werden sowohl gute Beispiele der IT-Sicherheit veröffentlicht als auch regionale und branchenspezifische Treffen zum Informationsaustausch organisiert. Ratsuchende finden hier viele Hinweise dazu, wie sich andere Unternehmen bereits gegen Bedrohungen aus dem Cyber-Raum wappnen. Nützliche Informationen bietet auch das Bundeskriminalamt in der Broschüre Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime.

Prävention in der EU, im Bund und den Ländern

40 Prozent der Wertschöpfung weltweit basieren bereits heute auf der Informations- und Kommunikationstechnologie. Weil IT-Infrastrukturen auch existentiell für das Funktionieren von Staat, Gesellschaft und Wirtschaft sind, gibt es die unterschiedlichsten Präventionsstellen auf EU-, Bundes- und

Länderebene. Die EU-Kommission hat Anfang 2013 einen Cybersicherheitsplan für Europa und eine Richtlinie für Netz- und Informationssicherheit vorgestellt. Im Januar 2013 eröffnete das „European Cybercrime Centre (EC3)“. Dieses „Europäische Zentrum zur Bekämpfung der Cyberkriminalität“. hat seinen Sitz in Den Haag. In Deutschland gibt es eine Cyber-Sicherheitsstrategie, deren Kern der Schutz kritischer Informationsstrukturen ist. Auf Bundesebene sind vier Stellen unter dem Dach des Bundesamts für Sicherheit in der Informationstechnik (BSI) für das IT-Krisenmanagement zuständig:

- CERT-Bund (Team für Bundesbehörden, bearbeitet Sicherheitsvorfälle, betreibt Warn- und Informationsdienst)
- IT-Lage- und Analysezentrum (bewertet die Sicherheitslage in Deutschland rund um die Uhr)
- IT-Krisenreaktionszentrum (schnelle Analyse, Koordination und Reaktionen bei Vorfällen)
- Nationales Cyber-Abwehrzentrum (NCAZ) – ein unter Federführung des BSI eingerichtetes, gemeinsam vom Bundeskriminalamt, der Bundespolizei, dem Zollkriminalamt, dem Bundesnachrichtendienst und der Bundeswehr betriebenes Zentrum zur Zusammenarbeit staatlicher Institutionen.

Direkte und unkomplizierte Hilfe erhalten Unternehmen auch auf Länderebene. So gibt es etwa in NRW das Cybercrime-Kompetenzzentrum NRW. In Niedersachsen ist die „Zentrale Ansprechstelle bei Cybercrime“ (ZAC) für diesen Bereich zuständig. Beim LKA BW ist seit Ende 2013 die Zentrale Ansprechstelle Cybercrime (ZAC) eingerichtet.
(ks) (25.07.2014)

Folgende Artikel könnten Sie auch interessieren:

- CEO-Fraud auf dem Vormarsch
- Wanzen im Wohnzimmer
- Gefälschte Stellenanzeigen
- Risikofaktor Plagiate
- Betrug beim Online-Gaming
- Marken- und Produktpiraterie

Alle Artikel dieser Kategorie

Weitere Infos zum Thema Diebstahl / Betrug

Profi-Anrufer bringen Senioren um ihr Geld

Betrügerische Callcenter-Mafia

Sie geben sich als Lotterieveranstalter, Polizisten, Rechtsanwälte...[mehr erfahren]

Drehen, fühlen, kippen

Falschgeld sicher erkennen!

Würden Sie sofort bemerken, wenn Sie einen gefälschten Geldschein in...[mehr erfahren]

Vor allem im Internet ist Vorsicht geboten

Sicher zum Gebrauchtwagen

Kaum eine Berufsgruppe wird so oft als Beispiel für unseriöses...[mehr erfahren]

Gefälscht wird, was gefällt

Professionelle Kunstfälschungen

Kunstfälschungen sind für Laien nicht einfach zu erkennen. Und selbst...[mehr erfahren]

Erst die Opfer ablenken, dann bestehlen

Video: Taschendiebe auf Beutezug

Wer von Giovanni Alecci beklaut wird, der hat Glück. Denn er ist ein...[mehr erfahren]

Cookie Einstellungen

□Statistiken
□Essentiell

Wir nutzen Cookies auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern.

Nur essentielle Cookies akzeptierenAlle akzeptieren