WER SIND DIE ANGREIFER? WIE GREIFEN SIE AN?

Im Jahr 2016 wurden deutschlandweit rund **83.000 Cybercrime-Fälle** mit einem **Schaden von ca. 52 Millionen Euro** zur Anzeige gebracht. Die Dunkelziffer liegt nach Aussagen der Ermittler weitaus höher. Die Angreifer sind u.a. Wirtschaftsspione, Cyber-Kriminelle, Cyber-Aktivisten, Skript-Kiddies, Nachrichtendienste, Militär, Cyber-Terroristen. Ihre Motivation ist v.a. finanzieller und vereinzelt extremistischer Natur. Lesen Sie, welche Phänomene die Cybercrime-Ermittler aktuell beschäftigen.

IDENTITY THEFT

Personenbezogene Daten werden missbräuchlich benutzt und Identitäten gestohlen bzw. Betrug ausgeübt. Der Angreifer verschafft sich über Social Engineering, Malware, Hacking und vorgetäuschten Websites Zugang zu Kreditkartendaten und persönlichen Informationen wie Anschrift und Geburtsdatum. So wird beispielsweise eine täuschendecht aussehende Rechnung an Kontakte aus privaten Adressbüchern gesendet.

DDOS-ERPRESSUNG (Distributed Denial-of-SERVICE)

Der Erpresser droht damit, einen Dienst zu überlasten oder zu beenden, sodass dieser nicht mehr nutzbar ist. Die Angriffe richten sich häufig gegen Webserver, d.h. Onlineshops und Internetdienstleister. Im Schadensfall drohen Image- und Einnahmeverluste. Wird auf das Erpresserschreiben nicht eingegangen, erfolgt u.U. ein Demonstrationsangriff. Laut LKA Sachsen geraten zunehmend auch Telefonanlagen mit IP-Telefonie ins Visier der Verbrecher.

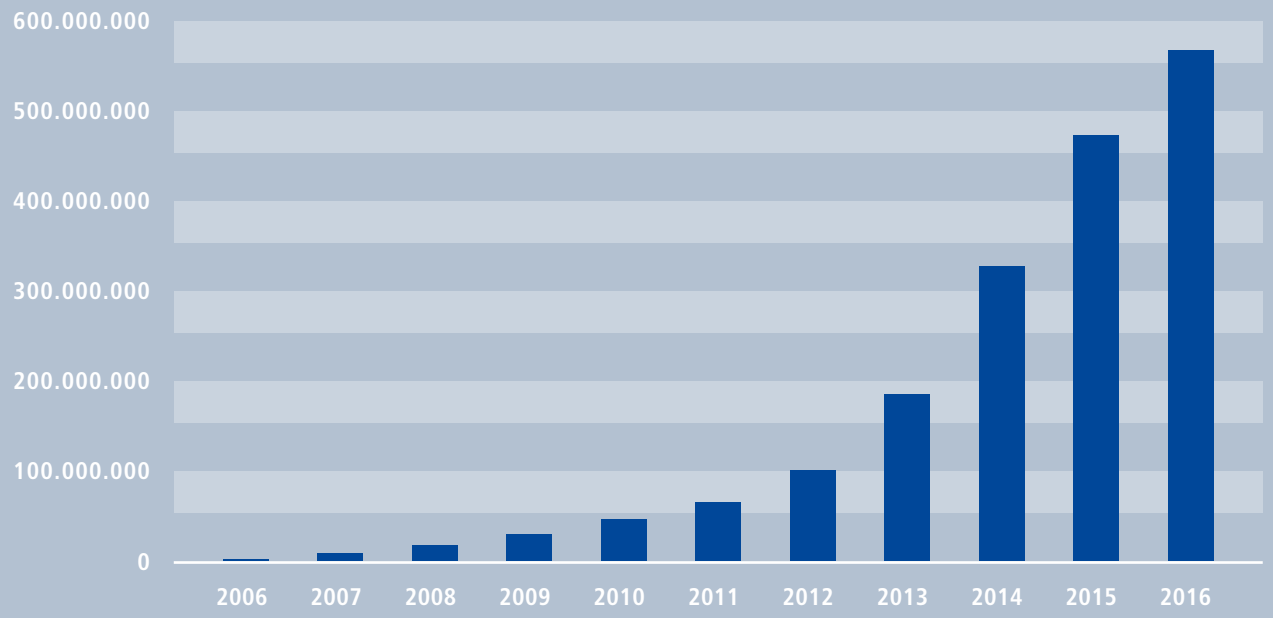
RANSOMWARE UND MALWARE

Ransomware beschreibt eine erpresserische Software, die den Zugriff auf eigene Dateien oder den Computer versperrt. Tritt häufig in Verbindung mit Malware, d.h. Schadsoftware wie Viren, Würmer, Trojaner und Spyware auf. Gedroht wird mit Vollverschlüsselung oder Systemsperrung. Der Angriff kann laut Erpresser nur gegen Zahlung (Bitcoin) vermieden werden.

Die Angriffswege sind vielfältig: E-Mails mit Anhängen, drive-by downloads, Serverschwachstellen, Fernwartungszugänge.

Es gibt Malware, die speziell für die Ausführung auf mobilen Geräten entwickelt wird. Vor allem für das Betriebssystem Android wurden ca. 15 Mio. verschiedene Malware gefunden, häufig verbreitet über Tauschbörsen. Neben den Datendiebstahl steht der Missbrauch (SMS-Versand, Anruf bei kostenpflichten Diensten) im Vordergrund.

Täglich werden 390.000 neue Schadprogrammvarianten identifiziert, insgesamt sind mehr als 560 Mio. Schadprogramme im Umlauf.



Bekannte Schadprogramme (2016 bis August), QUELLE: AV-TEST GmbH

CRIME AS A SERVICE

Kriminalität wird als Rund-um-Service im clear-web oder deep-web angeboten: die notwendige Malware ist auf illegalen Marktplätzen verfügbar. Darüber hinaus wird mit Zugangsdaten zu Online-Diensten, Kreditkartendaten und Dienstleistungen im Bereich Hacking, Technik, Sicherheit, Finanzen und Logistik gehandelt. Beratung und Betreuung runden das Paket ab. Somit ist für die Ausübung der Cyber-Straftaten ist keinerlei Expertise nötig. Die Akteure arbeiten häufig sogar arbeitsteilig zusammen.

CEO-FRAUD

Der Täter gibt sich als Mitglied der Geschäftsleitung aus und weist Mitarbeiter an, größere Geldbeträge ins Ausland zu überweisen. Die notwendigen Daten zu Firmenstrukturen, Mailadressen, Geschäftspartnern und Projekten werden vorab beispielsweise über Business Plattformen wie XING oder LinkedIn (Social Engineering) oder gezielte Telefonanrufe gesammelt. Seit 2013 gewinnt das Phänomen an Bedeutung: im Jahr 2016 wurden 291 Versuche registriert, von denen 51 für den Angreifer erfolgreich verliefen. Der reale Schaden belief sich auf 75,2 Mio. Euro.

SOCIAL ENGINEERING

Gehört zu den nicht-technischen Bedrohungen. Es bezeichnet das Umgehen von technischen Hürden durch die gezielte Beeinflussung von menschlichen Verhaltensweisen. Ziel ist die Preisgabe von Informationen, die Freigabe von Finanztransaktionen etc. Phising ist beispielsweise eine Form des Social Engineerings: hier versucht der Hacker über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten zu gelangen und Identitätsdiebstahl zu begehen.

QUELLEN: Cybercrime – Bundeslagebild 2016 mit freundlicher Unterstützung des Landeskriminalamts der Polizei Sachsen, Sophos Ltd., SHD System-Haus-Dresden GmbH

WAS TUN, UM SICH VOR ANGRIFFEN ZU SCHÜTZEN?

Ein möglichst **umfassender Schutz gegen Cyberangriffe** kann nur aus einem Zusammenspiel folgender Themenbereiche aufgebaut werden:

- **Funktionierende Schutzmechanismen am Gateway, im Netzwerk und am Client**
- **Sichere Datenspeicherung, -verwaltung und -verschlüsselung**
- **Implementierung und Zertifizierung von Informationssicherheitsmanagementsystemen (ISMS)**
- **Aufklärung und Sensibilisierung der Nutzer**

SHD konzipiert Ihnen passend zur Firmenstruktur und Ihren Geschäftsfeldern sowie Ihren Anforderungen im Bereich Compliance und Datenschutz eine sinnvolle Security-Gesamtlösung.

Wenden Sie sich gern an Thomas Beckert
Telefon: +49 351 4232-0
E-Mail: thomas.beckert@shd-online.de

SHD System-Haus-Dresden GmbH
Drescherhäuser 5b · 01159 Dresden
Telefon: +49.(0)351.42 32 - 0

www.shd-online.de