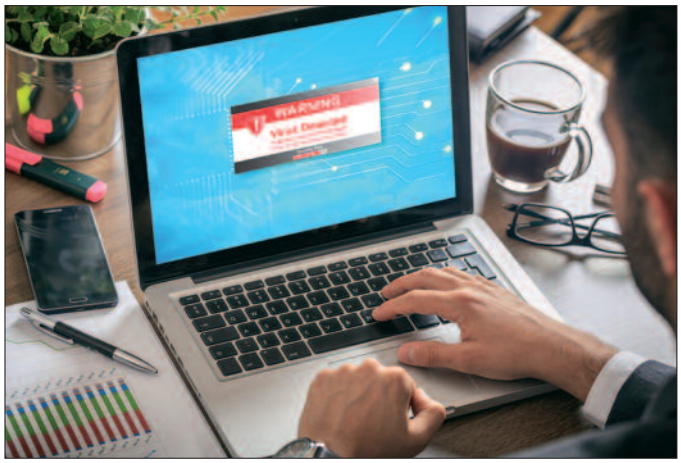


Verschlüsselungssoftware wird über präparierte E-Mails, Sicherheitslücken oder Herunterladen aus dem Internet verbreitet.

Spielzeug mit Funkverbindung: Geräusche in der Umgebung der Puppe werden heimlich an den Hersteller übertragen.

Online-Betrug und Erpressung

Das Bundeskriminalamt verzeichnete 2016 eine starke Zunahme der Zahl an Cybercrime-Delikten. Vor allem die Zahl der Fälle von Internetbetrug und digitaler Erpressung stieg an.

Die Zahl der Cybercrime-Delikte stieg um 30,9 Prozent von 10.010 Fälle 2015 auf 13.103 Fälle 2016. Zugenommen hat die Zahl der Fälle von Betrugsdelikten, Erpressungen, DDoS-Attacken und Hacking. Die Ursachen für den Anstieg liegen laut Polizei darin, dass die Täter immer stärker das Darknet nutzen, in der zunehmenden Verbreitung von Schadsoftware, dem mangelnden Gefahrenbewusstsein der Opfer sowie Schwächen in den IT-Systemen – wie zum Beispiel fehlende Sicherheitsupdates.

Digitale Erpressung durch Ransomware ist ein Dauerbrenner. Ransomware ist ein Sammelbegriff für Schadsoftware, die elektronische Daten und Systeme verschlüsselt, sodass diese nicht mehr verwendet werden können. Für die Entschlüsselung wird Lösegeld (englisch: ransom) erpresst, meistens in Form des virtuellen Zahlungsmittels „Bitcoin", das anonym ist und dadurch die Strafverfolgung erschwert. Die Verbreitung der Verschlüsselungssoftware erfolgt über präparierte E-Mails, durch Sicherheitslücken in Applikationen oder durch unbewusstes Herunterladen aus dem Internet („drive-by-download"). Davon betroffen waren 2016 neben Privatpersonen unter anderem Autohäuser, öffentliche und gemeinnützige Betriebe, Getränkehändler, Notare und Rechtsanwälte. Anfang 2016 wurden via E-Mails Empfänger verständigt, dass man ein Paket nicht habe zustellen können. Der Empfänger wurde aufgefordert, den Versandschein über einen Link in der E-Mail von der Internet-Seite des angeblichen Versenders herunterzuladen, um Gebühren zu vermeiden. Der Link verwies jedoch auf einen anderen Server. Bei der heruntergeladenen Datei handelte es sich um Schadsoftware. Eine abgewandelte Version solcher E-Mails hatte angebliche Rechnungen von Mobilfunkunternehmen oder Energieanbietern zum Inhalt. Die potenziellen Opfer sollten zum Herunterladen der Online-Rechnung verleitet werden.

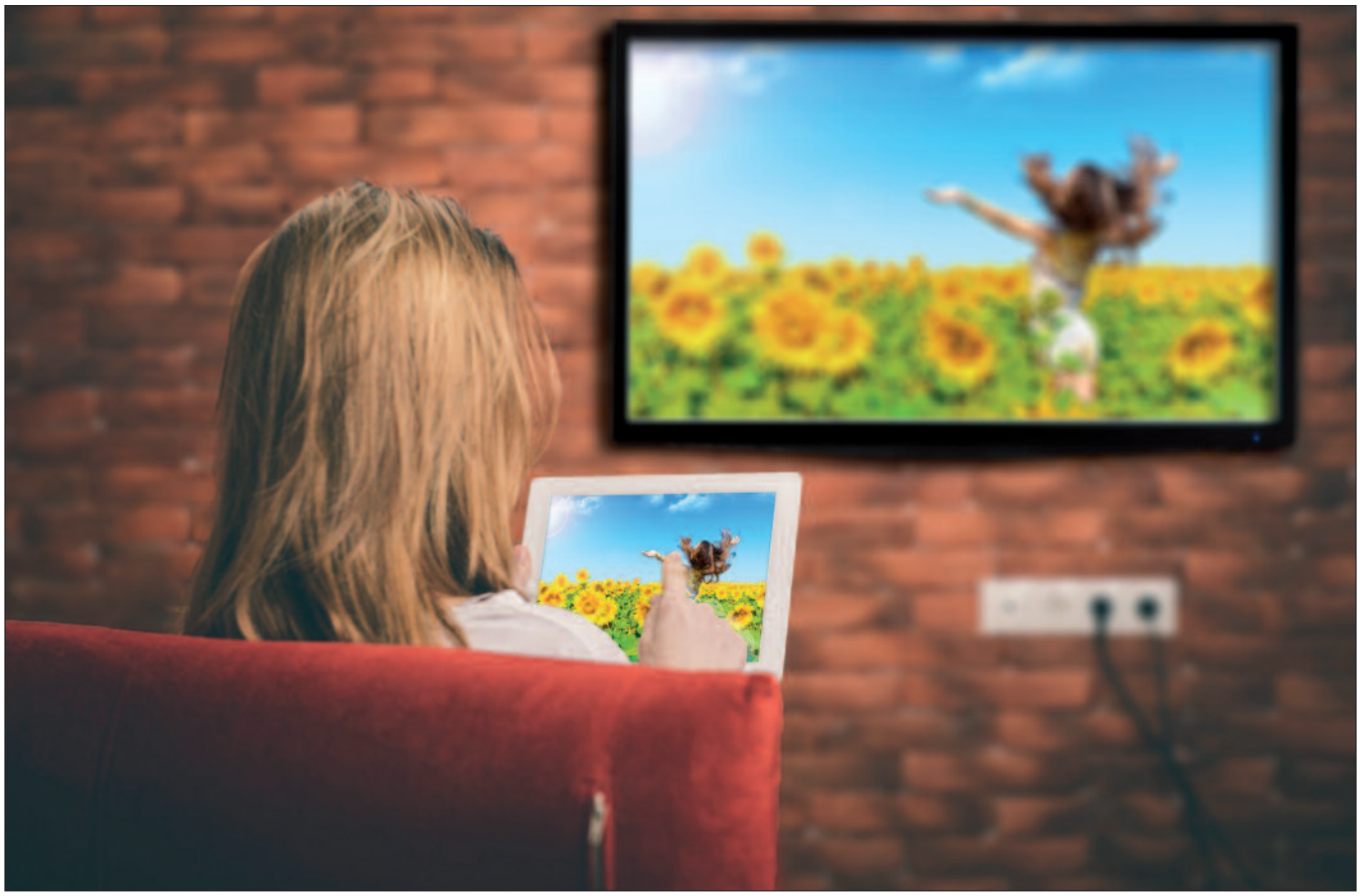
Schadsoftware wurde auch über gefälschte Bewerbungsschreiben verbreitet. Dabei wurde in den meisten Fällen in einem kurzen Anschreiben mit unterschiedlichen Absendern wie z. B. *julian.heyne@aon.at* auf weiterführende Unterlagen Bezug genommen. Der Download sollte zumeist von einer Dropbox erfolgen, manchmal war die Schadsoftware auch direkt an die Mail angehängt. Der E-Mail-Inhalt erschien glaubwürdig, die Gründe dafür, dass die Bewerbungsunterlagen nicht direkt beigelegt werden konnten, nachvollziehbar, was ein Erkennen der Gefahr erschwerte.

Zur Bekämpfung von Ransomware wurde im Juni 2016 im C4 die *Soko Clavis* eingerichtet. Ein Expertenteam aus IT-Technikern, Kriminalbeamten und Bitcoin-Spezialisten bearbeitete 2016 rund 480 Ransomware-Fälle für ganz Österreich. Von den in Österreich aufgetretenen über 30 Ransomware-Arten nahmen *Crypt0l0cker, CERBER* und *Locky* die Spitzenreiterrolle ein.

Bitcoin und virtuelle Zahlungsmittel. Sowohl technisch als auch rechtlich stellt die Verwendung von Bitcoins und anderen virtuellen Währungen eine Herausforderung für die Bekämpfung von Cybercrime dar. Die Geldflüsse aus Drogenhandel, Erpressung und anderen Straftaten erfolgen überwiegend auf diese Weise. Darüber hinaus bieten Dienstleister im Internet „Bitcoin-Mixer" an, um jegliche Verfolgung der Finanzströme zu unterbinden. Das deutsch-österreichische Projekt „Bitcrime" hat die Erforschung innovativer Lösungen zur Identifikation, Bekämpfung und Prävention der organisierten Finanzkriminalität mittels Kryptowährungen wie Bitcoins zum Inhalt. Die entwickelte Software wird bereits bei nationalen sowie internationalen Ermittlungsbehörden verwendet. Aufgrund der positiven Resonanz wird die Zusammenarbeit mit privaten und öffentlichen Forschungseinrichtungen in weiteren Projekten zum Thema Kryptowährungen intensiviert.

Cybercrime-as-a-Service (CCaaS). Kriminelle können Bausteine für Schadsoftware im Darknet bestellen. Ähnlich einem Fahrzeug-Konfigurator der Autohersteller können die gewünschten Ei-

Fotos: Rawf8/Fotolia, Fotogray71/Fotolia



Fernseher können sendefähige Kameras oder Mikrofone enthalten und Daten unbemerkt weiterleiten.

Foto: Rasulov/Fotolia

genschaften einer Schadsoftware ausgewählt und gekauft werden. Oft gibt der Hersteller eine Geld-zurück-Garantie, falls sie nicht funktioniert oder blockiert wird. Auch die Verteilung der Software nach Regionen oder Sprachen und das Waschen des Geldes werden angeboten. Neben Schadsoftware werden im Darknet auch DDoS-Attacken gestaffelt nach Dauer und Bandbreite des Angriffes zum Kauf angeboten. Bezahlt wird mittels Kryptowährung wie Bitcoin.

Hinter *Cybercrime-as-a-Service* stehen meist weit verzweigte, arbeitsteilig agierende Organisationen, die sowohl die erforderlichen Spezialistinnen und Spezialisten als auch Handlanger beschäftigen und bei einem Ausfall schnell für Ersatz sorgen. Die Strukturen sind jenen im Menschen- und Drogenhandel ähnlich.

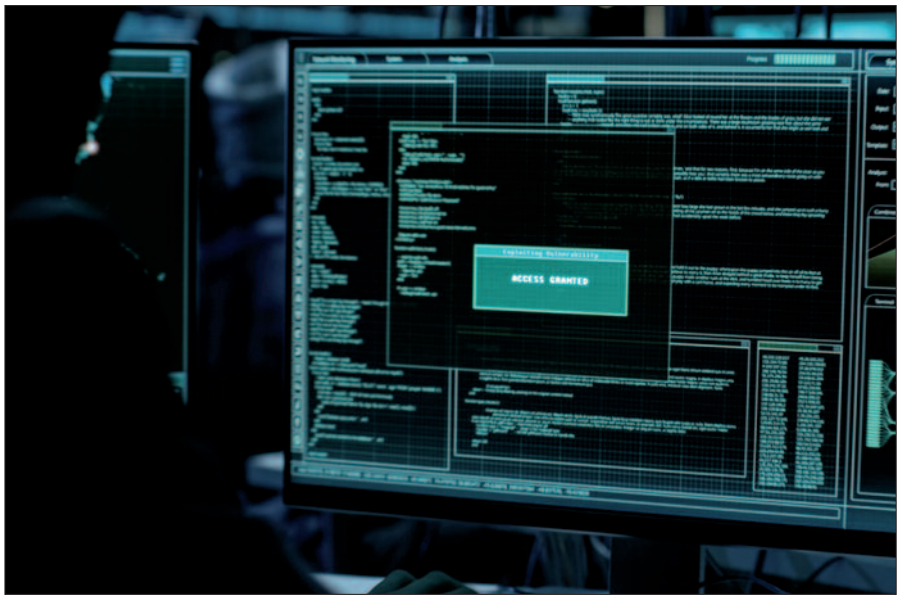
DDoS-Attacken. Im Gegensatz zu den weit gestreuten Wellen von Schadsoftware handelt es sich bei Distributed-Denial-of-Service-(DDoS)-Attacken um gezielte Angriffe. Sie stellen darauf ab, die Verfügbarkeit von Systemen und Ressourcen einzuschränken. Werden Webshops davon betroffen, die für Kunden nicht mehr erreichbar sind, kann dies den Ruin für das betroffene Unternehmen bedeuten. Sollte ein staatlicher Service davon betroffen sein und es zu Fristverlusten kommen, können weite Teile der Wirtschaft und auch Privatpersonen geschädigt werden. Die größte mediale Aufmerksamkeit erhielten 2016 die Angriffe auf das Telekomunternehmen *A1* und die *Zentralanstalt für Meteorologie und Geodynamik*.

Darüber hinaus gab es Angriffe auf Internetseiten von Unternehmen sowie öffentlichen Organisationen und Einrichtungen. In vielen Fällen folgten Drohungen, die Angriffe zu wiederholen, falls nicht eine bestimmte Summe bezahlt werden würde.

Internet of Things (IoT) bezeichnet die Vernetzung von Gegenständen über das Internet. Die vernetzten Geräte sind durchgehend online und können jederzeit angegriffen werden. Sie sind meist schlecht vor Gefahren geschützt, es fehlen Sicherheitsupdates. Bei vielen Geräten hat der Besitzer nicht die Möglichkeit zur Absicherung, da von den Herstellern keine Änderungen am System vorgesehen sind. Das *Internet of Things* birgt die Gefahr von Missbrauchs- und Angriffsmöglichkeiten, wie dem Aufbau von Bot-Netzwerken und DDoS-Attacken, Verbreitung von Malware sowie Phishing. Die Dunkelziffer ist hoch und die Gefahr für den Angreifer, entdeckt zu werden, ist gering.

Für den Privathaushalt werden Produkte angeboten, die per App kontrolliert und gesteuert werden können. Fernsehgeräte bieten die Möglichkeit, Filme über das Internet zu „streamen“. Bei einigen kann man über die eingebaute Kamera Videotelefonate führen oder sie reagieren auf Gesten und gesprochene Kommandos. Sprachsteuerungen lassen auch viele andere Funktionen zu, wie etwa das Licht ein- und auszuschalten, den Sender am Fernseher zu wechseln, Heizung oder Klimaanlage zu steuern, die Vorhänge zu schließen und vieles mehr. Selbst die Haustüre lässt sich inzwischen mittels einer App am Smartphone auf- und zusperren, wenn ein entsprechendes Schloss eingebaut ist.

Auch Puppen „verstehen“ und reagieren oder antworten. Da Spracherkennung eine hohe Rechenleistung erfordert, geschieht dies in der Regel nicht in der Puppe. Vielmehr werden alle Geräusche in der Umgebung der Puppe an den Hersteller übertragen, dort ausge-



Die Zahl der Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik nahm 2016 um 55 Prozent zu.

Projekt „Bitcrime“: Die Polizei verfolgt die Geldflüsse von Kriminellen.

wertet, die Reaktion der Puppe ermittelt und an die in Frage kommende Antwort zurückgesendet. Vorsicht geboten ist bei Bestellungen von Geräten im Billigst-Segment („China-Gadgets“), da die Gefahr besteht, dass bereits Hintertüren eingebaut sind.

Cybercrime-Meldestelle. Das *Cyber-Crime-Competence-Center (C^4)* im Bundeskriminalamt ist als nationale und internationale Zentralstelle für die elektronische Beweismittelsicherung und -auswertung zuständig, ebenso für Ermittlungen im Zusammenhang mit Cybercrime im engeren Sinn und die Koordinierung der Bekämpfung von Cybercrime. Im C^4 ist rund um die Uhr eine Meldestelle eingerichtet, die Meldungen über Cyber-Vorfälle aus der Bevölkerung, der Wirtschaft und der Polizei erhält. 2016 wurden mehr als 11.000 Mitteilungen und Hinweise aus der Bevölkerung sowie von in- und ausländischen Dienststellen und der Wirtschaft von der Meldestelle bearbeitet. Es ging vor allem um Ransomware und CEO-Betrug. Häufig wurden auch Fälle von Scheckbetrug bei Vorreservierungen aus dem Ausland, die Zustellung von ungerechtfertigten Rechnungen bei Eintragungen in Wirtschaftsdatenbanken oder der Domänenregistrierung gemeldet. Die Zahl der gemeldeten Fälle von Sextortion und ähnlichen Erpressungen ist 2016 im Vergleich zu den Vorjahren rückläufig.

Verstärkt wurde die Zusammenarbeit mit der Wirtschaft und Vereinen wie zum Beispiel der *Wirtschaftskammer Österreich (WKO)* oder der Initiative „Watchlist Internet“, um über aktuelle Phänomene zu informieren. Die Mitarbeiter der Meldestelle verschicken in einem Newsletter Warnmeldungen mit Handlungsempfehlungen an ausgewählte Multiplikatoren. 2016 wurden zehn Newsletter zu aktuellen Cyber-Phänomenen versandt.

Meldestelle für Kinderpornografie und Kindersextourismus. Die Zahl der Hinweise, die in der Meldestelle Kinderpornografie und Kindersextourismus im Bundeskriminalamt eingegangen sind, war 2016 rückläufig. 2015 gab es 2.742 Hinweise, davon 310 mit Österreichbezug; 2016 waren es 1.530 Hinweise, davon 347 mit Österreichbezug. Der Rückgang ist darauf zurückzuführen, dass Fotos und Filme vermehrt in geschlossenen Foren verbreitet werden. Die Zahl der Anzeigen wegen kinderpornografischer Darstellung Minderjähriger (§ 207a StGB) stieg von 465 im Jahr 2015 auf 681 im Jahr 2016; die Zahl der Anzeigen wegen Groomings (§ 208a StGB) stieg von 52 Anzeigen auf 80 Anzeigen. *Siegbert Lattacher*

CYBERCRIME

Mehr Anzeigen

Die Polizei unterscheidet zwischen Cybercrime im engeren Sinn und Cybercrime im weiteren Sinn. Cybercrime im engeren Sinn beschreibt jene Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden (z. B. Datenbeschädigung, Hacking, DDoS-Attacken). Unter Cybercrime im weiteren Sinne versteht man Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung und Ausführung für herkömmliche Kriminaldelikte eingesetzt wird, wie z. B. Betrugsdelikte, Kinderpornografie, Cyber-Grooming oder Cyber-Mobbing.

Die Zahl der Cybercrime-Delikte im engeren Sinn stieg um 55 Prozent von 1.696 (2015) auf 2.630 (2016). Die Zahl der Fälle von Cybercrime im weiteren Sinn nahm um 26 Prozent zu, die Zahl der Fälle von Internetbetrug (+ 2.200) stieg am stärksten an. Stark gestiegen ist die Zahl der Fälle von Datenbeschädigung (§ 126a StGB) – um 362 Prozent (+ 514) und der Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) – um 96 Prozent (+ 122).

Die Anzahl der Anzeigen wegen Hacking, dem unbefugten Eindringen in ein Computersystem (§118a StGB), stieg um 18 Prozent (70 Fälle). Die Aufklärungsquote sank von 41,5 Prozent auf 38,7 Prozent.

Foto: Cegli/Fotolia, Gorodenkoff/Fotolia