Unternehmen werden immer öfter von Ransomware bedroht. Der beste Schutz ist die Vorsicht der Mitarbeiter.

Digitale Erpressung

Schadsoftware, die Daten auf Computern und Smartphones verschlüsselt oder blockiert, breitet sich aus. Das Bundeskriminalamt hat eine Sonderkommission zur Bekämpfung dieser Delikte eingerichtet.

Ob Privatpersonen oder Unternehmen: Seit Jahren werden Nutzer mit Ransomware konfrontiert – entweder mit Schadprogrammen, die den Zugang auf mobilen Geräten blockieren, indem der Bildschirm mit einem speziellen Fenster überblendet wird, oder mit Schädlingen, die Daten auf Desktop-Computern verschlüsseln. Laut dem Softwarehersteller *Kaspersky Lab* stieg im ersten Quartal 2016 die Zahl neuer Ransomware-Modifikationen weltweit um 14 Prozent im Vergleich zum Vorquartal; die Zahl der von Verschlüsselungsprogrammen attackierten Nutzer stieg um 30 Prozent.

Soko Clavis. Aufgrund des Anstieges der Erpressungen durch Ransomware wurde Anfang Juni 2016 die Sonderkommission „Clavis“ im Cybercrime-Competence-Center (C[4]) des Bundeskriminalamts eingerichtet. Die Ermittlungsschritte, der internationale Bezug und die Auswertung von Spuren erfordern eine zentrale Aktenbearbeitung und Ermittlungstätigkeit. Die Soko-Mitarbeiter übernehmen bundesweit alle Ransomware-Fälle, die von den Kollegen in den Polizeiinspektionen aufgenommen werden. Digitale Spuren werden analysiert und mit den Datenbanken von Europol abgeglichen. Akte werden auf Gemeinsamkeiten und Zusammengehörigkeit geprüft, um Spuren zusammenzuführen. Aufgrund der vielen Spuren, die meist ins Ausland führen, sind staatsanwaltschaftliche und gerichtliche Anordnungen wie etwa Rechtshilfeersuchen zur Verfolgung der Täter notwendig.

Die Ermittler der Soko bearbeiten etwa 30 Fälle pro Woche. Die Ransomware „Cerber“ nahm im Sommer 2016 die Spitzenposition ein. Da „Cerber“ im europäischen Raum stark verbreitet ist, wurde bei der Europol eine *Joint Cybercrime Action Taskforce (J-CAT)* eingerichtet. Innerhalb dieser Taskforce werden die Erkenntnisse und Ermittlungsergebnisse auf internationaler Ebene zusammengeführt, verglichen und an der gemeinsamen Ausforschung der Täter gearbeitet.

In der vom österreichischen Bundeskriminalamt initiierten Europol-Taskforce hat die Soko „Clavis“ die Führungs- und Koordinationsrolle übernommen. Die Bezahlung des „Lösegeldes“ erfolgt meist mit der elektronischen Währung Bitcoin. Ein Soko-Mitarbeiter beschäftigt sich hauptsächlich mit der Analyse von Spuren. Gemeinsam mit einem Techniker werden Programme und Methoden zur Rückverfolgung des Geld-*Bitcoin*-Flusses entwi-

FOTO: CONTRASTWERKSTATT/FOTOLIA

ckelt. Eine Mitarbeiterin analysiert die technischen Abläufe innerhalb der einzelnen Ransomware-Netzwerke und koordiniert einen Großteil der nationalen Fälle.

Infizierung. Die Ransomware „Cerber“ zum Beispiel wird vor allem durch gefälschte Bewerbungsschreiben verbreitet. Die Täter antworten auf Stellenangebote im Internet und versenden den Schadcode mit den beigefügten Dateien, die beispielsweise als Lebenslauf getarnt sind. Dadurch verleihen sie ihren E-Mails Plausibilität. Betroffen sind vor allem Unternehmen.

Laut Ermittlern des Cybercrime-Competence-Centers im Bundeskriminalamt kann bei einem Befall mit „Cerber“ mit dem System weitergearbeitet werden, es werden nur die Nutzerdaten verschlüsselt. Beim Öffnen der verseuchten Datei wird der Schadcode ausgeführt bzw. aus dem Internet geladen. Betroffene werden in der Regel mit einer Bildschirmmeldung (Textdatei, Bilddatei, Bildschirmhintergrund) aufgefordert, Geld an die Angreifer zu übermitteln. Bei diesen Bildschirmmeldungen kann es sich entweder um einen Erpresserbrief handeln, es kann auch ein behördlicher Hintergrund vorgespiegelt werden (z. B. „Polizeiliche Sperre des Systems wegen Urheberrechtsverletzungen“).

Neben dem Öffnen eines manipulierten E-Mail-Anhangs oder dem Aufrufen eines vermeintlich harmlosen Links in einer E-Mail, der zu einer manipulierten Webseite führt, gibt es noch andere Gefahren, mit der „Erpressersoftware“ infiziert zu werden. Etwa durch den Besuch von vermeintlich harmlosen, jedoch manipulierten Webseiten. Der Virus wird dabei unbemerkt heruntergeladen (*Drive-by-Download*). Auch durch Ausführung eines bösartigen Makros in einem Office-Dokument kann man sich mit Ransomware infizieren.

Geld gegen Daten. Ist ein System mit Schadsoftware infiziert, werden die Daten verschlüsselt und können ohne den zugehörigen Schlüssel nicht mehr verwendet werden. Die Täter stellen in Aussicht, einen Schlüssel zu übermitteln, wenn die geforderte Summe (z. B. mit der Cryptowährung *Bitcoin* oder mit Prepaid-Karten) bezahlt wird. Experten von *Kaspersky Lab* raten davon ab, ein „Lösegeld“ zu zahlen, weil nicht garantiert ist, dass die Daten wieder entschlüsselt werden. Etwa im Fall der neuen Schadware *Ranscam* ist dieser Rat angebracht. *Ranscam* gibt vor, die Dateien auf eine „versteckte, verschlüsselte Partition“ verschoben zu haben. Die Dateien sind bereits gelöscht, bevor die Lösegeldforderung angezeigt wird und es gibt keine Möglichkeit sie wiederherzustellen.

Erpressung durch Datensperre: Die Täter stellen in Aussicht, einen Schlüssel zu übermitteln, wenn die geforderte Summe bezahlt wird.

Die Ransomware „Satana“ verschlüsselt Dateien, beschädigt den *Master Boot Record (MBR)* von *Windows* und blockiert den *Windows*-Bootvorgang. *Ded Cryptor* verlangt 2 Bitcoins (circa 1.200 Euro) als Lösegeld. Von *Ded Cryptor* betroffene Dateien können nicht entschlüsselt werden. Opfer können versuchen, die Daten von Schattenkopien wiederherzustellen, die vom Betriebssystem erstellt wurden.

Mobile Geräte. Die am weitesten verbreitete Art von Desktop-Ransomware ist der *Cryptolocker*. Für mobile Android-Geräte existieren fast keine *Cryptolocker*, weil die Betriebssysteme und Anwendungen Cloud-Back-ups erstellen. Wenn User ihre Dateien in der Cloud gesichert haben, gibt es keinen Grund, ein Lösegeld zu zahlen.

Blocker sind die bekannteste Methode, Android-Geräte zu infizieren. Der *Blocker* blockiert entweder Browser oder Betriebssysteme und fordert ein Lösegeld, um die Blockade aufzuheben. Auf Mobiltelefonen überdecken die Cyber-Kriminellen die Schnittstelle jeder App mit einem Fenster, so dass das Opfer keine Anwendung mehr benützen kann. PC-Besitzer können einen „Blocker“ relativ leicht loswerden. Sie müssen die Festplatte entfernen, sie auf einem anderen Computer anschließen und die Blocker-Dateien beseitigen. Bei einem Smartphone kann man nicht einfach den Hauptspeicher entfernen – er ist an die Hauptplatine gelötet.

Laut einer Studie von *Kaspersky Lab* über mobile Ransomware geht hervor, dass 23 Prozent der in Deutschland zwischen April 2015 und März 2016 angegriffenen Android-Nutzer von Ransomware attackiert wurden. Das ist eine Steigerung um das Fünffache im Vergleich zum Vorjahreszeitraum. Vier Malware-Familien waren für mehr als 90 Prozent der Attacken verantwortlich. Hierbei handelt es sich um die Schädlinge *Small, Fusob, Pletor* und *Svpeng*.

In Deutschland ist der mobile Erpressungstrojaner *Trojan-Ransom.AndroidOS-Fusob* sehr aktiv. Die Ransomware wird hauptsächlich über Pornoseiten als angeblich benötigter Multimedia-Player auf ein mobiles Gerät gebracht. Sie sammelt und verschlüsselt dort Daten und steht im Austausch mit den Angreifern, die dann das Gerät sperren können. Das geforderte Lösegeld beträgt zwischen 100 und 200 US-Dollar, bezahlbar mit *iTunes*-Gutscheincodes.

Im Vergleich zum PC-Bereich gibt es im mobilen Sektor mehr bildschirmsperrende Ransomware-Programme. Android-Nutzer können Bildschirmblocker nicht einfach mit Hilfe externer Hardware entfernen.

FOTO: NICESCENE/FOTOLIA

„Digitale Erpressung hat sich als Erfolgsmodell in der Cybercrime-Szene etabliert“, sagt Roman Unuchek, Mobile-Security-Experte bei *Kaspersky Lab*. „Auf Ransomware für den PC sind Erpressungsprogramme für mobile Geräte gefolgt. Anschließend werden wir Ransomware-Arten sehen, die es auf mit dem Internet verbundene Geräte wie Smart-Watches, Smart-TVs, aber auch auf Smart-Home-Systeme und Unterhaltungsanlagen im Auto absehen werden.“

Sicherheitstipps. Bei der Installation von Apps, die nicht aus den offiziellen App-Stores kommen, sollte man sehr vorsichtig sein. Eine aktuell gehaltene Sicherheitssoftware erkennt Schädlinge und gefährliche Webseiten. Wird eine App aus einem nicht offiziellen Store installiert, sollten Nutzer auf die eingeforderten Rechte achten. Gerade in diesem Fall ist der Einsatz einer mobilen Sicherheitslösung unverzichtbar. Nutzer

Bundeskriminalamt: Sonderkommission zur Bekämpfung von Ransomware.

sollten sich über Bedrohungen informieren. So minimiert sich das Risiko, unter anderem auf Social-Engineering-Attacken hereinzufallen.

„Ransomware ist deshalb so weit verbreitet, weil das dahinterstehende Geschäftsmodell sehr einfach ist: Gelangt ein Erpresserprogramm auf ein System, gibt es kaum eine Möglichkeit, den digitalen Erpresser loszuwerden, ohne dass persönliche Informationen verloren gehen“, erklärt Aleks Gostev, Sicherheitsexperte bei *Kaspersky Lab*. „Zudem erfolgt die Bezahlung des Lösegelds über *Bitcoins* anonym und ist kaum nachvollziehbar. Auch sehen wir immer häufiger Ransomware-as-a-Service-Geschäftsmodelle, bei denen Cyberkriminelle ein Entgelt für die Verbreitung von Malware oder einen Anteil des erpressten Lösegelds bei einem infizierten Nutzer bezahlen.“

Für einige Arten von Ransomware gibt es bereits eine Entschlüsselungssoftware. Diese wird meist kostenfrei von Antivirensoftware-Herstellern zur Verfügung gestellt. Die Täter entwickeln die Ransomware weiter und für die neuesten Varianten sind noch keine Möglichkeiten zur Entschlüsselung bekannt.

Auf *www.nomoreransom.org* finden Ransomware-Opfer Informationen, was Ransomware genau ist, wie die Schädlinge funktionieren und wie man sich davor schützen kann. Es gibt Tipps zur Wiederherstellung der Daten. *S. L.*

RANSOMWARE

Expertentipps

• Jedem Ransomware-Angriff geht eine Infektion voraus. Meist werden Social-Engineering-Techniken verwendet. Der beste Schutz ist die Vorsicht der Mitarbeiter.
• Schreibrechte von Mitarbeitern restriktiv handhaben. In der Regel ist eine Verschlüsselung von Daten nur dann möglich, wenn der jeweilige Benutzer über Schreibrechte verfügt.
• Software des Betriebssystems, Browser (einschließlich aller Plug-ins) und Sicherheitssoftware stets am aktuellen Stand halten.
• Download von potenziell gefährlichen Dateien (z. B. *exe, com, bat, vbs, msi, scr, js*) unterbinden.
• Den Empfang von verschlüsselten Containern (z. B. zip, rar) blockieren.
• Makros in Office-Dokumenten deaktivieren; die Ausführung von potenziell gefährlichen Codes (z. B. *JavaScript*) in PDF-Dateien vermeiden.
• Die Ausführung von Schadsoftware verhindern, indem man nur den Start von zuvor festgelegter Software auf „Whitelisting“- oder Signatur-Basis erlaubt; in jedem Fall die Ausführung von Dateien in *TEMP*-Ordnern unterbinden. Für den Mobilbereich sollte ausschließlich die Installation von Apps aus „offiziellen“ Quellen zulässig sein.

Back-up-Konzept

• In regelmäßigen Abständen Sicherungskopien der Daten erstellen. Ist es nicht vorgesehen, Back-ups von Clientrechnern zu erstellen, dann sollte (z. B. über die Gruppenrichtlinien) ein Netzwerklaufwerk als Default-Speicherort für Dateien eingerichtet sein.
• Das Sicherungsmedium nach der Sicherung von Daten aus dem Netzwerk entfernen. Ein Befall mit Ransomware kann oft auch alle erreichbaren Datenträger (z. B. Netzlaufwerke, externe Festplatten oder Back-up-Systeme) verschlüsseln.
• Das Back-up-Konzept regelmäßig testen. Oft erkennt man erst im Schadensfall, dass das Backupkonzept nicht ordnungsgemäß funktioniert.
• Wenn ein Mitarbeiter eine verschlüsselte Datei entdeckt, sollte unabhängig von einer etwaigen Back-up-Restore-Anforderung für diese Datei eine diesbezügliche Meldung an den Verantwortlichen im Unternehmen abgesetzt werden (oder bei der Back-up-Restore-Anforderung explizit auf diesen Grund hingewiesen werden). Anderenfalls werden weitere verschlüsselte Dateien nicht sofort gespeichert und künftig nur mehr im verschlüsselten Zustand gesichert.

Verhalten im Schadensfall

• Den betroffenen Client schnellstmöglich vom Daten-Netz trennen. Sofern die Verschlüsselung aller von diesem Client-Rechner erreichbaren Netzlaufwerken noch nicht abgeschlossen ist, kann dadurch möglicherweise ein Teil der Daten vor Verschlüsselung gerettet werden.
• Den betroffenen Client nicht vom Stromnetz trennen. Eventuell ist es mit Hilfe forensischer Maßnahmen möglich, nicht verschlüsselte Daten oder sogar den Schlüssel selbst aus dem Speicher auszulesen, solange der Rechner nicht vom Strom getrennt oder heruntergefahren wurde.
• Anzeige bei der Polizei erstatten.

Kontakt

Vorfälle können der Cybercrime-Meldestelle im Bundeskriminalamt gemeldet werden *(against-cybercrime-@bmi.gv.at)*.

Betreiber kritischer Infrastrukturen können sich auch direkt an das Cyber-Security-Center im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung wenden *(csc@bvt.gv.at)*.

FOTO: EGON WEISSHEIMER