Cybercrime nimmt zu

Täglich werden zahllose Cyberattacken gestartet. Die Schäden gehen in die Milliarden Euro. Wir unterhielten uns mit Dr. Philipp Amann von Europol über die neuesten Trends und wie man sich vor Malware schützen kann.

MARIO FRANZIN

Es ist wie im Wilden Westen. Cyberattacken nehmen sprunghaft zu. Den überrumpelten Opfern werden Konten geplündert, die Daten abgesaugt und ganze IT-Systeme lahmgelegt. Die in Österreich bekannten Fälle, wie FACC, die einem CEO-Fraud zum Opfer fiel oder Palfinger, deren IT-System über Wochen lahmgelegt wurde, ist nur ein kleiner Ausschnitt aus der Welt der Cyberkriminalität. Die Schäden durch unbefugten Zugriff auf Computersysteme und Endgeräte gehen mittlerweile in die Milliarden Euro.

Herr Dr. Amann, was sind die neuesten Entwicklungen in der Cyberkriminalität?
Was wir sehen, ist prinzipiell eine starke Zunahme der Aktivitäten. Das hängt einerseits damit zusammen, dass der Grad der Digitalisierung in allen Lebensbereichen stark zugenommen hat und sich damit mehr Angriffspunkte ergeben. Zum anderen formieren sich Cyberkriminelle zu schlagkräftigen Gruppen. Da haben wir es nicht mehr mit ein paar Jugendlichen zu tun, die irgendwo im Keller werken, sondern mit komplexen Organisationen. Wir sahen das, als wir das Netzwerk Emotet nach drei Jahren Ermittlung ausgehoben haben. Es ist uns 2014 das erste Mal durch eine kleine Schadsoftware aufgefallen. Nach drei Jahren wurden geschätzte 61 Prozent aller E-Mails mit Schadsoftware im Anhang über dieses Netzwerk verteilt. Die Kriminellen sind auch sehr agil. So griffen sie letztes Jahr das Thema Covid-19 sofort auf und benützten es als Thema für Spam-Emails.
Überdies bemerken wir, dass Internetkriminalität bereits als Crime as a Service angeboten wird. Es ist heute gar nicht mehr notwendig, als Krimineller über hohes technisches Know-how zu verfügen. Im Internet finden sich alle möglichen Tools und Services, die es Ihnen beinahe schon als Laien ermöglichen, Cyberattacken durchzuführen. Das weitet natürlich das Spektrum der Kriminellen deutlich aus.

Welche Art von Attacken sind derzeit am gängigsten?
Die meisten Fälle sehen wir derzeit bei Ransomware, bei der von Kriminellen Verschlüsselungssoftware installiert wird und damit Betriebsaktivitäten blockiert werden. Zum Teil werden die Daten vorher kopiert und weiterverkauft – das zentrale Ziel der Kriminellen ist aber letztendlich eine Geldforderung, die sie gegen eine Entschlüsselung der „gekaperten" Daten – zumeist über Kryptowährungen – stellen. Besonders in diesem Zusammenhang beschäftigen wir uns auch stark mit dem Thema Kryptowährungen.
Sehr häufig sind auch Phishing-Attacken mit dem Ausspähen von Kontodaten. Hier registrieren wir seit einiger Zeit eine starke Zunahme von Schadsoftware im Android-Bereich – also bei mobilen Endgeräten. Bei der Kompromittierung der Handys haben es die Kriminellen zumeist auf die darauf installierte Bankensoftware abgesehen. Manchmal kommt es sogar zum sogenannten SIM-swapping, was ein gutes Bespiel ist, wie Cyberkriminelle auf verbesserte Sicherheitsmaßnahmen reagieren. Dabei organisieren sich die Kriminellen beim Provider unter Vorspiegelung der Identität des Opfers eine neue SIM-Karte und empfangen damit die TAN-Codes für Überweisungen. Das Opfer merkt dies erst, wenn plötzlich der Handyempfang nicht mehr funktioniert. Da ist es aber meist schon zu spät und das Konto ist leergeräumt.

ZUR PERSON

Dr. Philipp Amann, MSc leitet die Strategieabteilung des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität (EC3). Die operativen und strategischen Schwerpunkte des EC3s sind High-Tech-Kriminalität, Betrug im Zahlungsverkehr, Darkweb-Kriminalität und Online-Kindesmissbrauch. Zu seinen Hauptverantwortungsbereichen gehören die vorausschauende Bewertung von Cyberrisiken und -bedrohungen, Technologiebewertung (z.B. 5G oder KI), die Planung und Umsetzung europaweiter Prävention und bewusstseinsbildender Maßnahmen und die strategische Kooperation auf EU-Ebene. Vor seinem Eintritt beim EC3 war Dr. Amann für den Bereich Cyberkriminalität bei der Organisation für Sicherheit und Zusammenarbeit in Europa zuständig. Dr. Amann ist promovierter Wirtschaftsinformatiker und schloss seinen MSc im Bereich Forensic Computing and Cybercrime Investigation am University College Dublin ab. Er publizierte auch u.a. zu den Themenbereichen Cybersicherheit, Cyberkriminalität, internationale Ermittlungsverfahren, elektronische Beweismittelverwaltung, Digitale Forensik sowie Datenstandards.

Dr. Philipp Amann: „Mit jedem Erfolg, den die Kriminellen erzielen, steigen deren Motivation und deren technische Möglichkeiten."

Häufiger als man liest, kommen auch CEO-Frauds vor. Bei dieser Form des Betrugs gehen die Kriminellen sehr konsequent vor. Sie spähen das Zielunternehmen über Wochen aus, bringen die personelle Hierarchie in Erfahrung und fahren dann die Attacke unglaublich überzeugend – in Einzelfällen wurden neue Methoden des Deep Fake eingesetzt, bei denen gefakte personelle Identitäten sehr real vorgespiegelt werden können.

Zu den Ransom-Angriffen: „Pay or not to pay?" ist im Falle des Falles die Frage. Sie raten den Unternehmen, prinzipiell kein Lösegeld zu bezahlen …

Ja, das stimmt. Obwohl mir natürlich bewusst ist, dass das oft für das betroffene Unternehmen eine betriebswirtschaftliche Entscheidung ist. Aber man muss bedenken, dass die Kriminalität mit jeder Zahlung gefördert wird. Außerdem ist nicht gesichert, dass man trotz Lösegeldzahlung seine Daten zurückerhält. Und selbst wenn, dauert es oft Tage oder unter Umständen Wochen, bis die Daten wieder einsatzfähig sind. Außerdem führen Kriminelle oft Listen, auf denen Sie als potentielles Opfer nach oben wandern. Wenn Sie einmal Lösegeld gezahlt haben, erhöht das damit die Wahrscheinlichkeit, dass später wieder ein Angriff auf Sie gestartet wird – Sie haben ja beim ersten Mal bereits bezahlt. An dieser Stelle möchte ich auf eine unserer Initiativen hinweisen. Unter nomoreransom.org bieten wir kostenfrei etwa 100 verschiedene Tools an, mit denen eine große Anzahl von bekannter Ransomware entschlüsselt werden kann. In den ersten vier Jahren seit Bestehen dieser Initiative haben wir es geschafft, rund 630 Millionen Euro an Lösegeldforderungen zu stoppen!

Es gibt Versicherungen gegen Schäden durch Cyberkriminalität. Raten Sie dazu?

Versicherungen befinden sich hier prin- ››

> „Cyberkriminalität ist keine Revolution, sondern eine Evolution."

zipiell auf einem schwierigen Gebiet. Auf der einen Seite ist es für die Versicherungsnehmer von Vorteil, weil die Versicherungen vor der Übernahme einer Deckung Sicherheitschecks der IT-Umgebung und deren dahingehende Optimierung voraussetzen – und damit das Risiko verringern. Auf der anderen Seite glaube ich, dass Versicherungen oft dazu geneigt sind, einem Lösegeld zuzustimmen, da die Übernahme der Lösegeldforderung oft günstiger ist als der Schaden durch einen längeren Betriebsstillstand oder einen größeren Datenverlust. Damit können sie aber ungewollt diese Form der Cyberkriminalität fördern. Wir erlebten auch schon, dass sich Hacker die Daten von Versicherungsunternehmen besorgten und dann gezielt jene Unternehmen angriffen, die eine Cyberversicherung abgeschlossen hatten – da das die Zahlungswilligkeit erhöhen kann. Die AXA hat sich mittlerweile von der Versicherung solcher Schadensfälle distanziert und bietet sie nicht mehr an.

Was sind derzeit die Hauptangriffspunkte bei Cyberattacken?

Ein unterschätzter Schwachpunkt sind oft die Menschen bzw. Mitarbeiter in den Unternehmen. Dem kann man vor allem durch Schulungen vorbeugen. Wenn Mails mit Phishingsoftware geöffnet werden, ist den Kriminellen zumeist schon Tür und Tor geöffnet. Datenverluste bzw. missbräuchliche Verwendung bis hin zum Verkauf der Daten im Darknet sind oft die unmittelbare Folge. Ein sensibler Bereich sind oft auch Endgeräte, z.B. im medizinischen Bereich.

Wie kann man sich gegen diese Art der Kriminalität schützen?

Im Prinzip gibt es keinen 100-prozentigen Schutz dagegen, aber dennoch kann man präventiv viel tun – bereits erwähnt habe ich die Mitarbeiterschulung, man kann auf der technischen Seite z.B. Antiviren Software verwenden, bekannte Softwareschwachstellen schließen, effiziente Firewalls installieren, unbenützte Ports schließen, Mehrfachauthentifizierungen einsetzen etc. Wichtig ist auch ein gutes Backupregime, das man immer wieder testen sollte. Es ist schon vorgekommen, dass man im Schadensfall feststellen musste, dass ein Backup aufgrund von Speicherplatzmangel nur einen Teil der Daten gesichert hat. Daher immer wieder einen Test aufs Exempel machen!

Wenn ich nun Opfer einer Cyberattacke geworden bin, wie kann mir Europol dann helfen?

Wir haben ein umfangreiches internationales Netzwerk aufgebaut – sowohl im operativen Bereich mit der Joint Cybercrime Action Taskforce (J-CAT) als auch mit Beratungsgruppen speziell für den Finanz-, den Telekom- und den Cybersicherheitsbereich. Drei Mal pro Jahr treffen wir einander und beraten über die aktuellen Entwicklungen und mögliche Lösungen. Besonders die internationalen Kooperationen sind für uns ein wichtiger Aspekt, da die Kriminellen oft länderübergreifend agieren. Letztes Jahr konnten wir gemeinsam über 35 komplexe Fälle abschließen – u.a. wurde das bereits erwähnte kriminelle Netzwerk Emotet unschädlich gemacht.

Es ist absolut wichtig, im Akutfall die Behörden zu informieren. Bei einer Meldung über eine nationale Behörde an uns, können wir dann konkrete Unterstützung anbieten, um z.B. zu verstehen, wie es zu dem Eindringen der Kriminellen ins System gekommen ist. Eine Aufarbeitung des Schadens dauert aber in der Regel mehrere Wochen – oft auch, nachdem bereits Lösegeld bezahlt wurde. Es ist nicht auszuschließen, dass dann bereits sensible Daten gestohlen wurden. Manche Kriminelle sind derart unverfroren, und weisen das Opfer darauf hin, dass sie bei einer Meldung des Datenverlustes Probleme mit der Datenschutzbehörde bekommen würden – das soll die Verschwiegenheit und die Bereitschaft, Lösegeld zu zahlen, erhöhen. Zum Teil gibt es aber genau eine solche Meldepflicht, vor allem aus Datenschutzgründen!

Sollten Sie weiteres Interesse am Thema Cybersecurity haben, wir veröffentlichen u.a. jedes Jahr einen Bericht (IOCTA) über die aktuelle Lage. Dieser steht auf unserer Homepage zum Download zur Verfügung.

www.europol.europa.eu/ec3

NOMENKLATUR

Botnet: Ein Computernetzwerk mit einem Kommando- und Kontrollzentrum zum Versenden von Spams oder um DDoS-Angriffe durchzuführen.

Rootkit: Eine Sammlung von Programmen, die den Zugriff auf einen Computer oder ein Computernetzwerk auf Administratorebene ermöglicht.

Wurm: Repliziert sich über ein Computernetzwerk und führt selbstständig böswillige Aktionen aus.

Trojaner: Stellt sich als legitimes Programm dar, ist aber für kriminelle Zwecke wie Ausspionieren, Datendiebstahl, Löschen von Dateien oder Erweitern eines Botnetzes konzipiert.

Backdoor/Remote-Access Trojan (RAT): Greift aus der Ferne auf ein Computersystem oder mobiles Gerät zu. Es kann durch eine andere Malware installiert werden und gibt dem Angreifer fast die vollständige Kontrolle, der dann eine Vielzahl von Aktionen ausführen kann (Überwachung, Senden von Dateien und Dokumenten an den Angreifer, Protokollieren von Tastenanschlägen usw.).

Ransomware: Blockiert den Zugriff auf das Gerät und fordert ein Lösegeld, um den Zugriff wieder zu ermöglichen.

Scareware: Ist eine gefälschte Antiviren-Software, die vorgibt, zu scannen und eine Malware auf dem Gerät des Benutzers zu finden, die sie gegen Bezahlung entfernt.

Spyware: Überwacht die Aktivitäten des Benutzers und leitet die Informationen an Dritte weiter.

Adware: Zeigt Werbebanner oder Pop-ups an, die Codes enthalten, um das Verhalten des Benutzers im Internet zu verfolgen.