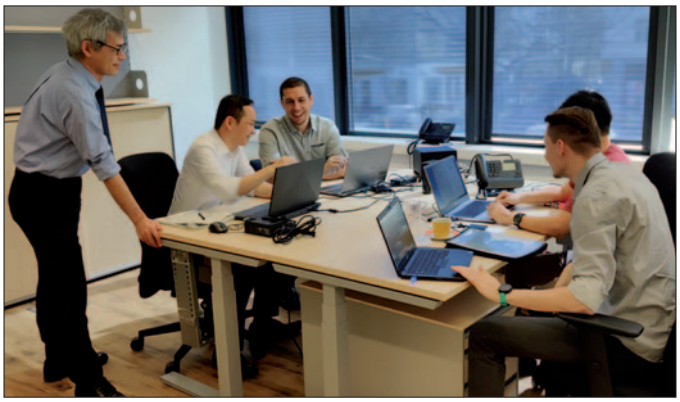
Ransomware-Angriffe entschlüsselt

Ransomware-Angriffe auf Unternehmen richten weltweit nicht nur große Schäden an, sondern stellen auch für die Polizei eine Herausforderung dar. Durch internationale Kooperationen konnten verschlüsselte Daten aus Ransomware-Angriffen entschlüsselt und den Opfern geholfen werden.

Mittwochmorgen: Ein blinkender Hinweis erscheint auf dem Firmen-Laptop eines Unternehmers. Die Schreckensnachricht: Die Fabrik steht still, die Maschinen funktionieren nicht und die Mitarbeiterinnen und Mitarbeiter haben keinen Zutritt zum Gebäude. Es vergeht nicht viel Zeit und schon melden sich die ersten Kunden mit Fragen und Beschwerden. Die Firma ist Opfer eines Ransomware-Angriffes geworden. Cyber-Kriminelle haben sich Zugang zum IT-System verschafft und den gesamten Datenbestand mit einer Schadsoftware verschlüsselt. Im hinterlassenen Erpressungsschreiben fordern die Täter die Zahlung einer hohen Summe für die Entschlüsselung der Daten. Doch gibt es keine Garantie, dass die Daten nach der Bezahlung von den Tätern entschlüsselt werden.



Mitarbeiter des Cybercrime-Competence-Centers mit Kollegen der japanischen Polizei in Wien

Steigende Zahl an Ransomware-Fällen. Ransomware-Angriffe auf Unternehmen sorgen weltweit für große Schäden und stellen eine der größten Bedrohungen für die Cyber-Sicherheit dar. Die Qualität der Angriffe steigt kontinuierlich und wenn sich diese als erfolgreich erweisen, sind die Reaktion und Aufarbeitung zeit- und kostenintensiv. Die Vorgehensweise bei Ransomware-Angriffen hat sich von der Ausgangslage geändert. Anfangs handelte es sich um einfache Lösegeldforderungen, die sich 2022 zu einer Multifaktor-Erpressung entwickelten. Die Daten werden beim Angriff nicht mehr nur verschlüsselt, sondern auch durchforstet und exfiltriert, um den Opfern anschließend mit der Veröffentlichung der Daten im Internet oder Übermittlung an ein Konkurrenzunternehmen zu drohen. Die Angriffe erfolgen zum Teil über E-Mails mit einer Schadsoftware als Anhang oder durch das Nützen von Sicherheitslücken. Die von den Tätern geforderten Geldbeträge liegen zwischen wenigen Tausend Euro und bis zu zweistelligen Millionenbeträgen. 2022 wurden österreichweit 181 Fälle zur Anzeige gebracht.

Ermittlungen gegen Ransomware-Angriffe. Das Referat IT-Ermittlungen (vormals Soko Clavis) des *Cybercrime-Competence-Centers (C4)* im Bundeskriminalamt koordiniert und ermittelt schwerpunktmäßig Ransomware-Fälle in ganz Österreich. Da sich Ransomware-Angriffe nicht auf nationale Gebiete beschränken, ist eine internationale Zusammenarbeit notwendig.

Europol-Verbindungsbeamte Ko Ikai aus Japan und Christopher Rauch aus Österreich

Zusammenarbeit zwischen C4 und japanischer Polizei. Die international agierende Ransomware-Gruppe „LockBit“, die für den Angriff auf acht österreichische Unternehmen verantwortlich war, wurde Gegenstand von Ermittlungen. Von den Ransomware-Angriffen waren Unternehmen in zahlreichen Ländern betroffen, unter anderem in Japan. Wenn gleichartige Fälle in vielen Ländern auftreten, schließen sich Verbindungsbeamtinnen und -beamte bei Europol im Wege der *Joint Cybercrime-Action-Taskforce (J-CAT)* zu eigens eingerichteten Operationen zusammen. Die Zusammenarbeit zwischen dem *C4* und der japanischen Polizei begann damit, dass der Cybercrime-Verbindungsbeamte des Bundeskriminalamts bei Europol, Christopher Rauch, und der japanische Verbindungsbeamte bei Europol, Ko Ikai, Überschneidungen bei den Ermittlungen zur LockBit-Gruppe feststellten und das Potenzial einer Kooperation in diesem Fall erkannten. Nach einem Informationsaustausch beschlossen Japan und Österreich zusammenzuarbeiten, weshalb Cyber-Ermittler aus Japan für eine Woche im *C4* in Wien zu Gast waren. In tagelanger Arbeit wurden Analysen durchgeführt, wobei gegenseitige Erfahrungen und Expertisen ausgetauscht wurden. Ein erheblicher Teil des Datenmaterials konnte entschlüsselt und der Schaden eines der betroffenen Unternehmen reduziert werden. „Cyber-Kriminelle agieren international, weshalb wir auch eine sehr gute internationale Vernetzung und Zusammenarbeit benötigen“, erklärt Klaus Mits, Leiter der Abteilung 5 (Kriminalpolizeiliche Assistenzdienste) im Bundeskriminalamt.

Ransomware-Gruppierung „HIVE“. 2022 formierte sich bei Europol eine internationale Operation mit mehreren

FOTOS: THOMAS KIRCHBERGER/EUROPOL, RAPHAEL STRASS/BK

Polizeibehörden, um gegen die Ransomware-Gruppierung „HIVE“ zu ermitteln. „HIVE“ ist eine russischsprachige Hackergruppe, die vor allem durch Ransomware-Angriffe auf Krankenhäuser und öffentliche Einrichtungen bekannt wurde. Sie soll für mehr als 1.500 Cyberangriffe verantwortlich gewesen sein, darunter 3 in Österreich. Die Gruppe bot Ransomware-as-a-Service an und soll durch Erpressungen über 100 Millionen US-Dollar (92 Mio. Euro) verdient haben. Die Gruppe wurde im Juni 2021 entdeckt. 2022 gelang es amerikanischen Sicherheitsbehörden die Server und Webseiten der Gruppe zu konfiszieren. Sie stellten dabei den Entschlüsselungsschlüssel der benützten Programme sicher. Die Europol-Ermittlungsgruppe kontaktierte die Ermittlungsbehörden jener Länder, in denen sie Opfer der HIVE-Gruppe identifiziert hatten.

Die Polizei in Österreich konnte den Geschädigten das spezifische Entschlüsselungstool zur Verfügung stellen und somit Daten retten. „Wir erfahren oft aufgrund von Ermittlungen oder von im Darknet von Hackern geleakten Informationen über Unternehmen oder Organisationen, dass sie Opfer eines Ransomwareangriffs geworden sind. Es meldet sich nicht automatisch jede betroffene Firma bei uns, obwohl wir ihnen unsere Hilfe anbieten“, sagt einer der Ermittler des *Cybercrime-Competence-Centers* im Bundeskriminalamt. Entschlüsselungen von gesperrten Daten oder Computersystemen sind nicht immer einfach, denn es hängt von verschiedenen Faktoren ab und es ist nicht gewährt, dass ein System erfolgreich wiederhergestellt werden kann.

Lösegeldforderungen. „Die Empfehlung ist, dass Sie kein Lösegeld zahlen sollten. Wenn Sie Geld an Cyber-Kriminelle überweisen, bestätigen Sie ihnen, dass ihr ‚Geschäftsmodell’ funktioniert und es gibt keinerlei Garantie, dass Sie nach der Bezahlung die Entschlüsselungssoftware erhalten. Erstatten Sie unbedingt Anzeige bei der Polizei und treffen Sie im Vorfeld geeignete Gegenmaßnahmen“, sagt Abteilungsleiter Mits.

Mehr Informationen über die Funktion von Ransomware und wie Sie sich davor schützen können, finden Sie auf der Website von „No More Ransom“ *(www.nomoreransom.org)* *R. T.*