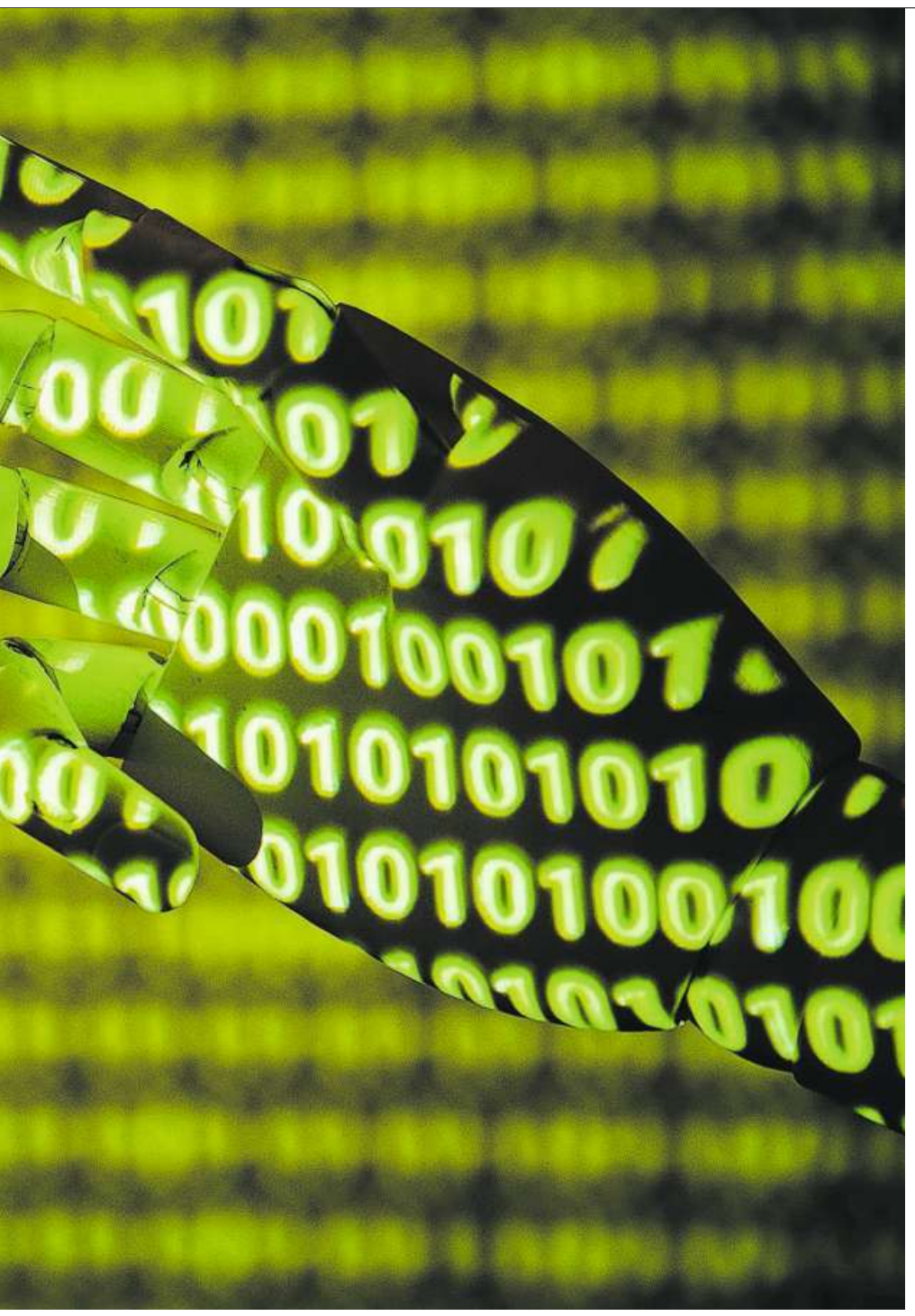


len zu einer existenziellen Gefahr für eine Firma, wenn sie keine Aufträge mehr bearbeiten, keine Kontakte mehr abrufen und keine Löhne mehr auszahlen kann. So bleibt häufig kein anderer Ausweg, als Lösegeld zu zahlen.

Gleichzeitig wird so das Geschäftsmodell der Hacker-Banden alimentiert. Das Lösegeld erlaubt es Cyberkriminellen, eine Infrastruktur von Hackern und anderen Gehilfen wie Geldwäscher zu finanzieren. So hat sich in den letzten Jahren eine Industrie von Cyberkriminalität entwickelt, die mutmasslich Milliarden umsetzt. Rund 70 Ransomware-Gruppen sind weltweit aktiv. Darum raten die Behörden dringend davon ab, den Erpressern nachzugeben und auch nur einen Franken zu zahlen. Es gibt einen zweiten Grund, wieso die Behörden davon abraten: Es gibt keine Sicherheit, dass die Angreifer weg sind, dass sie die Daten nicht doch noch veröffentlichen wollen und die Erpressung somit weitergeht.

Wenig Mittel gegen wachsende Kriminalität

Das Perfide an der Situation: Die Risiken für die Kriminellen sind beschränkt. Gemäss der aktuellen polizeilichen Kriminalstatistik können immerhin 34,4 Prozent der digitalen Delikte aufgeklärt werden. Allerdings gilt das vorab für Betrug. Bei Ransomware-Angriffen liegt die Aufklärungsquote bei 1,3 Prozent.

Die Strafverfolgung entpuppt sich in den meisten Fällen als schwierig bis unmöglich. Die Kriminellen agieren häufig aus dem Ausland. Die Polizeien sind daran, die Schlagkraft zu verbessern. Die Konferenz der Kantonalen Polizeidirektoren (KKJPD) will zusammen mit dem Bund unter anderem die Strafverfolgung stärken. Dazu soll eine nationale Übersicht über Cybervorfälle erstellt, die Ausbildung der Strafverfolgungsbehörden im Bereich Cyberkriminalität weiter verbessert und die Zusammenarbeit der Strafverfolgungsbehörden stärker ausgebaut werden. Doch schon beim ersten Punkt, der Übersicht über Cybervorfälle, hadern die Politiker auf nationaler Ebene. Es gibt bis heute keine Meldepflicht für Cyberattacken. Immerhin hat letzte Woche das Parlament entschieden, dass zumindest die Angriffe auf kritische Infrastrukturen gemeldet werden müssen. Weitergehende Meldepflichten wollte der Ständerat aber nicht.

Sowohl für die Polizeien als auch für das NCSC steht die Prävention im Vordergrund. Seit Jahren wird vor Hackerangriffen und ihren schwerwiegenden Folgen auch für KMU gewarnt. 2021 stellte das NCSC fest, dass die Warnungen versandeten und die Empfehlungen zum Schutz vor Angriffen nicht «flächendeckend umgesetzt» werden.

Die Sensibilisierung steigt langsam – auch weil unterdessen viele Unternehmen einschlägige Erfahrungen machen mussten.

Wer steckt hinter «Play»?

Die ersten Angriffe startete die weltweit aktive Hackergruppe «Play» im vergangenen Sommer. Die Wahl der Opfer der Gruppe erscheint willkürlich: Darunter befinden sich unter anderem etliche Schweizer Firmen, die Stadtverwaltung von Oakland in Kalifornien, eine Regionalbank in Spanien sowie eine argentinische Justizbehörde. Auch die Mediengruppen NZZ und CH Media, zu der diese Zeitung gehört, wurden jüngst von «Play» angegriffen. Wer genau hinter «Play» steckt, ist nicht bekannt. Ebenso unklar ist das Land, von dem aus die Gruppe operiert. Allgemein gilt Russland als Stützpunkt von Cyberkriminalität: Gemäss einer Analyse der US-Firma Chainalysis flossen 2021 rund 74 Prozent der erpressten Gelder an Gruppen mit Russland-Bezug. Dies entspricht mehr als 400 Millionen Dollar.

Zwei amerikanische IT-Sicherheitsfirmen haben das Vorgehen von «Play» technisch untersucht: Demnach dürfte es eine personelle Verbindung zu «Hive» geben, jener Gruppe, die für mehr als 1500 Cyberangriffe in über 80 Ländern verantwortlich gemacht wird und im Januar 2023 zerschlagen wurde. *(nma)*

«Momentan gibt es zu viele Opfer»

Tobias Ellenberger, Chef der Cybersicherheitsfirma Oneconsult, verrät, wie die Hackergruppen vorgehen und wieso sie mittelgrosse Firmen angreifen.

Ann-Kathrin Amstutz

Wie suchen Ransomwaregruppen wie «Play» ihre Opfer aus?
Tobias Ellenberger: Es gibt zwei typische Angriffsmethoden. Bei der ersten benutzen die Cyberkriminellen gestohlene Zugangsdaten, die bei einem Leck erbeutet wurden. Die Daten werden dann für Phishing-Attacken benutzt – oder um sich direkt im System einzuloggen. Diese Methode benutzt «Play» sehr häufig. Bei der zweiten Variante, mit der «Play» anfänglich bekannt wurde, nutzen die Hacker bekannte Schwachstellen aus, wie etwa die zwei Sicherheitslücken auf den Microsoft «Exchange»-Mailservern. Über diese hat die Gruppe Angriffe auf verschiedene Firmen gestartet.

Das klingt weniger nach gezielten Angriffen.
Es kommt im Zuge von Ransomwareattacken selten vor, dass Firmen ein ganz bestimmtes Unternehmen ins Visier nehmen. Meistens nutzen sie veraltete Software oder gestohlene Daten grossflächig aus – mit dem Ziel, dass daraus möglichst viele Opfer resultieren.

In den letzten Tagen war in den Medien von mehreren erfolgreichen Angriffen zu lesen. Also ist auch dort nicht von gezielten Angriffen auszugehen?
Was den initialen Zugriff betrifft, sind es erfahrungsgemäss meistens die typischen Angriffe, die erfolgreich sind. Zurzeit werden oft Fernzugriffszugänge über VPN, die teils ungenügend abgesichert sind, als initialer Zugriff verwendet. Entweder weil gültige Zugangsdaten erbeutet wurden oder aber weil die eingesetzte VPN-Software Schwachstellen aufweist, die noch nicht «gepatcht», das heisst durch Softwareupdates behoben, wurden. Bei Letzterem kommt es oft darauf an, wer schneller ist: die Entwickler und die Unternehmen oder die Hacker.

Und das sind dann wohl meist die Kriminellen.
Von den anderen Fällen hört man halt nichts. Diejenigen, die genug schnell waren, die trifft es nicht.

Sind denn Schweizer Firmen besonders häufig von Cyberangriffen betroffen?
Nein. Es gibt aber gewisse Trends: Ganz grosse Firmen sind seltener betroffen, unter anderem weil sie mehr Geld in die Sicherheit investieren. Zudem haben sie Hilfsmittel, um Angriffe schnell zu entdecken, sodass es nicht zu einem flächendeckenden Ausfall kommt. Deshalb zielen die Angreifer eher auf mittelgrosse Firmen. Alle Länder, in denen Oneconsult aktiv ist (Schweiz, Deutschland, Österreich und Neuseeland, die Red.), sind etwa gleich stark betroffen. Da die Angriffe oft in Wellen erfolgen, gibt es manchmal regionale Peaks. Jüngst haben wir das in skandinavischen Ländern beobachtet, ein andermal sahen wir einen Peak im deutschsprachigen Raum.

Dann täuscht der Eindruck nicht, dass die Gruppe «Play» gerade besonders aktiv ist. Befinden wir uns in einer solchen Welle?
Es gibt momentan drei Gruppen, die relativ aktiv sind: Play, Lockbit und Black Cat. Diese sind aber sehr schwer voneinander abzugrenzen, weil es Kriminelle gibt, die für mehrere Gruppen arbeiten. Da kann man auch Ähnlichkeiten in der Schadsoftware entdecken, etwa zwischen «Play» und der mittlerweile zerschlagenen Gruppe «Hive».

Also gibt es Kriminelle, die von einer Gruppe zur nächsten gewechselt sind?
Selbst wenn den Behörden ein Schlag gegen eine Gruppe gelingt, ist es meist nicht so, dass alle Täter erwischt und eingesperrt werden. Meist kann nur ein Teil der Infrastruktur lahmgelegt werden. Vielleicht bleiben die Entkommenen eine Zeit lang inaktiv und feilen an ihrer Schadsoftware, um dann unter anderem Namen wieder aufzutauchen. Sie können damit so viel Geld machen, dass sie nicht einfach so aufhören.

Wie eine Hydra: Wenn man einen Kopf abschlägt, wachsen zwei neue nach.
Es geht in diese Richtung. Das «Geschäftsmodell» ist einfach zu lukrativ. Die Gruppen sind dezentral organisiert. Sie haben teils Hunderte von Mitarbeitenden und sind professionell aufgestellt – mit Stellvertretungen und einem diversifizierten Geschäftsmodell. Sie rechnen damit, dass ein Teil geschnappt und ausgehoben wird. Ransomwaregruppen sind nichts anderes als organisierte Kriminalität.

Und sie sind damit sehr erfolgreich …
Momentan gibt es wirklich zu viele Opfer. Es ist bei uns in den Verhandlungen mit Täterschaften schon vorgekommen, dass sie sagten: Ihr müsst jetzt warten, wir haben zu viele Opfer. Sie waren schlicht überlastet.

Was ist denn angesichts dieser Lawine zu tun?
Das Risiko, erwischt zu werden, muss für die Kriminellen massiv steigen, damit ihr Modell weniger attraktiv wird. Sie wägen – wie legale Unternehmen auch – das Risiko gegen den Ertrag ab. Man muss also die Sicherheit flächendeckend erhöhen. Auch die internationale Strafverfolgung muss noch besser koordiniert werden. Dann gibt es ein typisches Katz-und-Maus-Spiel.

Wie können sich Firmen präventiv schützen?
Zum einen muss man es den Kriminellen möglichst schwer machen, die Infrastruktur eines Unternehmens zu knacken. Zum anderen sollte man so gut vorbereitet sein, dass man im Falle eines Angriffs möglichst schnell reagieren kann. Da hilft es zu wissen, wie die Kriminellen operieren, um die nächsten Schritte vorauszusehen.

Ist man da nicht abhängig davon, wie gut Softwareanbieter wie Microsoft ihre Systeme und Clouds schützen?
Jein. Es kann sein, dass ein Anbieter eine Lücke zu langsam schliesst. Dann ist der potenzielle Schaden grösser, weil über die Cloud potenziell mehrere Firmen betroffen sind. Dafür haben die grossen Cloudanbieter viel mehr Geld und Knowhow, um ein Abwehrdispositiv aufzuziehen. Beispielsweise könnte sich ein KMU, das eine Cloud benutzt, die entsprechenden Sicherheitsmassnahmen im Eigenbetrieb gar nicht leisten. Jede Firma muss für sich abwägen, was für sie die sicherste Lösung ist. Die Verantwortung liegt am Schluss bei der Firma selbst.

Und was raten Sie Firmen, die mit einer Lösegeldforderung erpresst werden?
Idealerweise ist man so gut auf diesen Fall vorbereitet, dass man andere Optionen hat als eine Zahlung. Ich würde aber nicht pauschal sagen, man sollte nie zahlen. Teilzahlungen können ein taktisches Mittel sein – etwa, um sich Zeit zu verschaffen oder um mit der Polizei zu schauen, auf welche Konten das Geld geht. So lässt sich die Schlinge um die Tätergruppen zuziehen. In Extremfällen kann es sein, dass man zahlen muss, um die Firma zu retten. Eine Lösegeldzahlung sollte aber sicher eine der allerletzten Massnahmen sein.

Viele Angriffe werden aber gar nie öffentlich. Sollte es für Firmen eine Meldepflicht geben?
Eine Meldepflicht ist hilfreich, um ein gutes Gesamtbild über die Lage zu erhalten und um anderen Opfern effizient zu helfen. Die Frage ist: Wann muss die Meldung erfolgen? Es kann strategische Gründe geben, einen Angriff nicht sofort zu melden – etwa, wenn ein Hacker im System noch aktiv ist und noch nicht gemerkt hat, dass er entdeckt wurde. Im Nachhinein ist es aber sicher gut, die Erkenntnisse zu teilen und daraus zu lernen.

Wie gut sind Schweizer Firmen denn gewappnet?
Die Situation ist je nach Branche sehr unterschiedlich. Es gibt sicher Nachholbedarf. Nicht alle Firmen haben ihre Hausaufgaben gemacht, sonst gäbe es nicht so viele Opfer. Das zeigt sich etwa an der Microsoft «Exchange»-Schwachstelle: Der Bund hat Briefe verschickt an betroffene Unternehmen, doch es gibt immer noch verwundbare Firmen, die die Schwachstelle noch nicht behoben haben. Daran müssen wir arbeiten.



«Es gibt derzeit drei Gruppen, die relativ aktiv sind: Play, Lockbit und Black Cat.»

Tobias Ellenberger
CEO Oneconsult