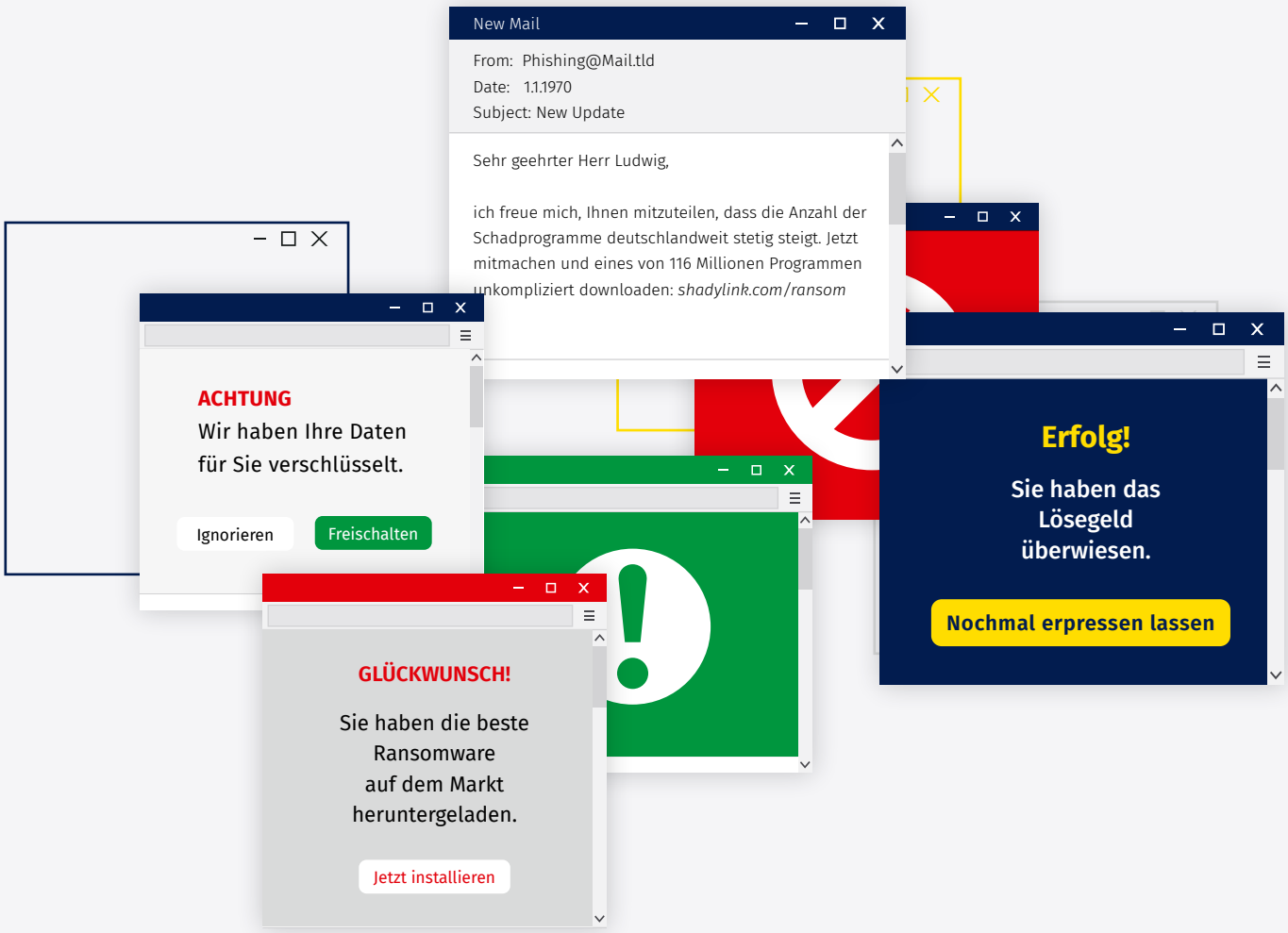

Serviceorientierte Cyberattacken

INTERVIEW Alexandra Resch

Die Zeiten der holprig getexteten Erpresserschreiben sind vorbei. Heute gehen Kriminelle bei Cyberattacken sehr userfreundlich vor. Was das für die Bekämpfung bedeutet und wie Betroffene im Ernstfall reagieren sollten, diskutieren Isabel Münch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und Dr. Michael Meier, Inhaber des Lehrstuhls für IT-Sicherheit am Institut für Informatik der Universität Bonn.

Im Gespräch waren sich BSI-Expertin Isabel Münch und Cybersecurity-Forscher Michael Meier einig: Neue Tools und alte Systeme machen es Kriminellen heutzutage besonders einfach, Angriffe mit Ransomware durchzuführen.

> ***„Die Hersteller sind in der Regel sehr schnell damit, Patches für Schwachstellen in ihren Produkten zu entwickeln. Aber bis diese in den Systemen von Unternehmen und Institutionen eingespielt werden, vergeht oft wertvolle Zeit.“***
>
> ISABEL MÜNCH

Was beschäftigt Sie aktuell am BSI, Frau Münch?

ISABEL MÜNCH Was Sicherheitsvorfälle angeht, sind Ransomware-Angriffe weiterhin das, was uns am meisten umtreibt. Es gibt Schwachstellen ohne Ende, sowohl in Produkten – also Programmen, die auf den Geräten genutzt werden – als auch in Systemen, die zum Beispiel schlecht konfiguriert sind. Aber die Angriffe selbst haben sich in den vergangenen Jahren stark gewandelt.

Wer kennt mein Passwort?
Mit dem Leakchecker der Uni Bonn kann jede und jeder überprüfen, ob die eigenen Zugangsdaten von Diebstahl betroffen sind:
leakchecker.uni-bonn.de

Inwiefern?

IM Vor ein paar Jahren liefen Ransomware-Angriffe in der Regel so ab, dass Systeme verschlüsselt wurden und dadurch zum Beispiel ein Unternehmen nicht mehr auf seine Daten zugreifen konnte. Um diesen Zugriff zurückzubekommen, musste ein Entschlüsselungsschlüssel gekauft werden. Heute setzen Kriminelle häufig auf Double Extortion – also zweifache Erpressung: Sie kopieren die Daten, bevor sie sie verschlüsseln. So können sie auch noch damit drohen, Geschäftsgeheimnisse oder Kundendaten zu veröffentlichen. Mit dieser Methode werden gerade zahlreiche Institutionen angegriffen.

MICHAEL MEIER Hinzu kommt, dass Phishing und der Missbrauch von dabei gestohlenen Passwörtern weiterhin eines der wichtigsten Einfallstore für diese Angriffe ist. Und durch Tools wie ChatGPT ist es mittlerweile ganz einfach, eine gute Phishing-Mail zu verfassen oder eine entsprechende Website zu erstellen. Wir forschen schon seit 2016 zu diesem Thema und staunen immer wieder über die schieren Mengen an Zugangsdaten, die in kriminellen Kreisen kursieren.

Wie viele davon konnten Sie bisher ausfindig machen? Und was geschieht damit?

MM Tatsächlich liegen uns aktuell über 25 Milliarden Datensätze vor. Bei acht Milliarden Menschen auf dem Planeten ist das erst mal schwer zu glauben, aber wenn man bedenkt, wie viele unterschiedliche Dienste wir im Alltag nutzen, ist das gar nicht überraschend. Mit unserem Leakchecker kann jeder überprüfen, ob seine Zugangsdaten betroffen sind. Über die Ausgründung Identeco beliefern wir verschiedene Anbieter, darunter etwa Xing oder Payback, mit den gesammelten Informationen, um es Kriminellen so schwerer zu machen, auf die Benutzerkonten dieser Services zuzugreifen.

IM Wir vom BSI informieren zudem möglichst umfassend und so schnell wie möglich über Schwachstellen, die in bestimmten Produkten entdeckt wurden. Die Hersteller sind in der Regel sehr schnell damit, Patches für eine solche Schwachstelle zu entwickeln, aber bis diese in Systemen von Unternehmen und Institutionen eingespielt werden, vergeht oft wertvolle Zeit.

Woran liegt das?

IM Ein Beispiel: Vor anderthalb Jahren haben wir eine Warnung über eine Schwachstelle in Servern von Microsoft Exchange herausgegeben, ein in Deutschland weitverbreitetes Produkt. Mit dieser Warnung sind wir bis in die Tagesschau gekommen. Danach haben wir beobachtet, was wir in diesen Fällen immer beobachten: In den ersten Tagen nach der Veröffentlichung sind sehr viele Systeme gepatcht worden, 20 Prozent aber eben auch nicht. Damit diese letzten Schwachstellen ausgeräumt werden, braucht es viel Information und Überzeugungsarbeit. Häufig ist den Admins durchaus bewusst, dass dieses Problem existiert, aber sie bekommen von der Business-Abteilung nicht das Go, das System für einen ganzen Tag vom Netz zu nehmen, um das Update einzuspielen.

> ***„Kriminelle gehen heute sehr serviceorientiert vor. Da gibt es Callcenter und Eins-zu-eins-Support, um Schritt für Schritt dabei zu helfen, das Lösegeld zu bezahlen. Auch was die Höhe der geforderten Summe angeht, wird genau recherchiert, wo die Schmerzgrenze liegt.“***
>
> MICHAEL MEIER

Zuletzt waren vermehrt Cyberattacken auf Hochschulen in den Medien. Warum werden gerade die angegriffen?

IM Kurz gesagt: weil es geht. Wir nennen das Opportunität. Mögliche Attacken werden heute zuerst in der Breite ausprobiert und dann gezielter eingesetzt. Manche Opfer sind schlicht und ergreifend Ausgangspunkt für weiterführende Angriffe. Bei vielen Hochschulen ist es leider auch zu einfach, Zugriff auf ihre Systeme und damit auf sehr viele Daten zu bekommen.

Wie läuft so ein Angriff in der Regel ab?

IM Mit dem klassischen Erpresserschreiben, das man aus dem Fernsehkrimi kennt, hat das auf jeden Fall nichts mehr zu tun. Als Erstes öffnet sich meistens ein Hinweisfenster auf dem angegriffenen Rechner: ‚Wir haben festgestellt, dass Ihr Server unzureichend geschützt ist. Aus Sicherheitsgründen haben wir Ihre Daten verschlüsselt …‘ Und dann kommt die erste Zahlungsanforderung. Durch diesen Prozess wird dann sehr kundenfreundlich durchgeführt.

MM Das kann ich bestätigen. Kriminelle dieser Art gehen heute sehr serviceorientiert vor. Da gibt es Callcenter und Eins-zu-eins-Support, um den Betroffenen Schritt für Schritt dabei zu helfen, das Lösegeld zu bezahlen. Und dieses verlangen sie nicht direkt in Bitcoin, sondern bieten handelsübliche Wege über Vermittler an, um die Erpressten nicht zu überfordern. Auch was die Höhe der geforderten Summe angeht, wird vorab genau recherchiert, wo die Schmerzgrenze eines Unternehmens liegt.

Wohl wissend, dass nicht jeder Angriff gleich ist: Gibt es grundsätzlich Empfehlungen, wie mit einer Cyberattacke umzugehen ist?

IM Unsere erste Empfehlung ist immer: Don’t panic. Ruhe bewahren. Die zweite wäre eigentlich: Holen Sie Ihren Notfallplan aus der Schublade, auf dem für verschiedene Szenarien genau beschrieben ist, welche Schritte als Nächstes zu befolgen sind. Das ist die Grundlage eines funktionierenden Sicherheitsmanagement-Systems und legt in der Regel auch direkt fest, welche Personen Teil des Notfallteams sind, das man in so einer Situation unbedingt braucht: eine kleine Gruppe von Mitarbeitenden, die aus dem Tagesgeschäft aussteigen und sich sofort dem konkreten Notfall widmen. Dann gilt es zu klären: Wer ist für was zuständig – und wer gerade nicht? Wer übernimmt welche Aufgaben? Und auch ganz wichtig: Wer muss informiert werden?

Damit meinen Sie Behörden?

IM Ja, für viele Institutionen ist es gesetzlich verpflichtend, in so einem Fall die Behörden einzuschalten. Oft ist es auch einfach angeraten. Zudem haben heutzutage viele Unternehmen Cyberversicherungen, die natürlich ebenfalls informiert werden müssen. Ebenso die Kunden oder andere potenziell Betroffene. Teil der Vorbereitung auf den Ernstfall muss es daher auch sein, die entsprechenden Kontaktdaten so zu hinterlegen, dass man sie auch noch findet, wenn die eigenen Systeme verschlüsselt sind.

Herr Meier, gibt es weitere Entwicklungen, die Sie beobachten?

MM Gerade beschäftigen wir uns sehr stark mit sogenannten Software Supply Chain Attacks, die in den vergangenen Jahren stark zugenommen haben. Hintergrund ist, dass Software heute nicht mehr von einer Organisation eigenständig gebaut wird, sondern aus vielen Komponenten besteht, die von unterschiedlichen Menschen und Unternehmen entwickelt wurden – und dann auch in verschiedenen Produkten zum Einsatz kommen. Wenn es Kriminellen nun gelingt, ein solches Puzzleteil zu manipulieren, dann sind damit automatisch alle Softwareprodukte kompromittiert, die dieses als Komponente einsetzen.

Eine Abschlussfrage: Fühlt sich die Arbeit im Bereich IT-Sicherheit manchmal nach Sisyphus und Stein an?

MM Für mich bleibt es auf jeden Fall spannend, immer wieder neue Veränderungen zu beobachten und darauf zu reagieren. Frustrierend finde ich – vielleicht eine überraschende Aussage von einem Informatiker –, dass wir so schnell von einer Technologie-Generation zur nächsten wechseln. Da ist meiner Ansicht oft zu sehr der Fokus auf Profit, als auf Nachhaltigkeit.

IM Ich gebe Herrn Meier recht: Es bleibt immer spannend. Und so richtig stimmt das Bild vom Sisyphus auch nicht. Denn für uns ist es nicht immer derselbe, sondern immer wieder ein neuer Stein.

Deep Dive

Für alle, die tiefer in die Materie einsteigen wollen, haben die beiden Interviewten ein paar zusätzliche Leseempfehlungen zusammengestellt:
inf.gi.de/to/cyberattacken

Isabel Münch ist Fachbereichsleiterin IT-Sicherheitslage am Bundesamt für Sicherheit in der Informationstechnik (BSI). Sie ist Gründungsmitglied der GI-Fachgruppe Sicherheitsmanagement, kurz SECMGT, und wurde 2015 als GI-Fellow ausgezeichnet.

Prof. Dr. Michael Meier ist Inhaber des Lehrstuhls für IT-Sicherheit am Institut für Informatik der Universität Bonn und Leiter der Abteilung Cyber Security bei Fraunhofer FKIE. In der GI hat er die Fachgruppe Security – Incident Detection and Response, kurz SIDAR, gegründet und ist bis heute als Sprecher der Gruppe aktiv.