Cyber-Kriminalität

Malware aus dem Online-Shop

[30.05.2022] Kritische Infrastrukturen standen im vergangenen Jahr erneut stark im Visier von Cyber-Kriminellen. Das ist ein Ergebnis des Bundeslagebilds Cybercrime 2021 des Bundeskriminalamts (BKA). Weitere Erkenntnis: Ransomware-Angriffe werden immer gefährlicher. Was können Unternehmen und Behörden tun, um sich zu schützen?

Am 5. Juli 2021 fiel die Landkreisverwaltung Anhalt-Bitterfeld einem schweren Cyber-Angriff zum Opfer. Die Bereitstellung öffentlicher Dienstleistungen war nach der Ransomware-Attacke nachhaltig eingeschränkt. Die in Sachsen-Anhalt gelegene Kommune rief den Katastrophenfall aus. Ein Novum. Auch Monate nach dem Angriff war noch kein Regelbetrieb möglich.
Der Cyber-Angriff auf den Landkreis Anhalt-Bitterfeld war ein besonders spektakulärer Vorfall unter vielen. Laut dem aktuellem Bundeslagebild Cybercrime 2021, den das Bundeskriminalamt (BKA) jetzt vorgestellt hat, standen Kritische Infrastrukturen (KRITIS) und Behörden im vergangenen Jahr besonders im Visier von Angreifern. Grund für die vermehrten Angriffe auf KRITIS ist, dass diese eine ungemein wichtige Bedeutung für das staatliche Gemeinwesen haben und auf einen reibungslosen Betrieb ihrer IT-Systeme angewiesen sind. Dementsprechend kann ein erfolgreicher Angriff zu einer gesellschaftlichen Notlage und drastischen Auswirkungen auf die Zivilbevölkerung führen, wenn beispielsweise die Strom- und Wasserversorgung oder die öffentliche Sicherheit akut gefährdet sind. Das macht sie leicht erpressbar. Hinter solchen Angriffen stecken in den meisten Fällen so genannte Ransomware-Attacken – also Erpressungsangriffe, die Daten verschlüsseln oder abziehen und dann ein Lösegeld fordern. Die Zahl der Erpresserangriffe hat laut BKA 2021 weiter zugenommen. Gleichzeitig ist der jährliche Schaden durch Ransomware in den vergangenen Jahren rasant gestiegen: von 5,3 Milliarden Euro im Jahr 2019 auf circa 24,3 Milliarden Euro im Jahr 2021. Der durchschnittliche Schaden pro Attacke hat um 21 Prozent zugelegt.

Dramatisch verschärfte Gefährdungslage

Der Ransomware-Trend ist nicht neu – doch die Gefährdungslage verschärft sich aktuell dramatisch. Dass Ransomware immer gefährlicher wird, hat unterschiedliche Ursachen.

1. Die Malware gibt es im Online-Shop: Für Kriminelle wird es immer einfacher, Erpressungsangriffe zu starten. Denn die dafür benötigte Malware kann inzwischen jeder auf einschlägigen Seiten im Internet erwerben. Durch ein solches Ransomware-as-a-Service-Angebot steigen die Verbreitung und die Professionalisierung der Angriffe weiter an.
2. Phishing wird immer professioneller: Personenbezogene Daten können bereits für geringe Summen erworben werden. Phishing-E-Mails lassen sich dadurch immer realistischer gestalten. Für die Mitarbeitenden eines Unternehmens wird es nahezu unmöglich, kriminelle E-Mails zu enttarnen. Das ist extrem gefährlich für die Unternehmen: Denn Phishing gehörte 2021 zu den Haupteintrittsvektoren für Schad-Software – auch von Ransomware.
3. Fake-E-Mails schüren die Angst: Phishing-E-Mails zum Thema Covid-19 haben 2021 zwar abgenommen, doch Phishing-Nachrichten nehmen noch immer häufig Bezug auf aktuelle gesellschaftliche Entwicklungen, so das BKA. Vor allem aber versuchen sie, Unsicherheiten der Empfänger auszunutzen oder eine Angstkulisse aufzubauen. Dies gelingt etwa durch knappe Zeitfristen oder Androhung von

Geldstrafen. Die am häufigsten für Phishing imitierten Absender waren 2021 Microsoft, DHL, Amazon, Google und WhatsApp.
4. Die Erfolgsquote steigt: Die Abhängigkeit von digitalen Daten ist in Unternehmen und Behörden stark gewachsen. Unternehmen sind daher eher bereit, auf die Forderungen von Erpressern einzugehen. Ein wichtiger Hebel für die Digitalisierung war das Homeoffice: Es liegen heute deutlich mehr Daten auf Behörden-/Unternehmensservern ab, als dies vor der Pandemie der Fall war.
5. Das Erpressungsgeschäft wird immer lukrativer: Daten werden bei Ransomware-Angriffen längst nicht nur verschlüsselt, sondern auch von den Systemen gestohlen. Auf diese Weise lassen sie sich weiterverkaufen. Außerdem können Hacker Schweigegeld einfordern, wenn sie androhen, diese zu veröffentlichen. Auch Kunden der eigentlichen Opfer werden damit erpresst, dass Ihre Daten veröffentlicht werden, sollte keine Zahlung erfolgen.
6. DDoS verschärft Erpressungen: Zusätzlich zur Datenverschlüsselung und -veröffentlichung legen immer mehr DDoS(Distributed Denial of Service)-Attacken die Web-Seiten der Opfer lahm. Im Jahr 2021 hat das BKA verstärkt Multivektor-Angriffe, so genannte Carpet-Bombing und eine Kombination von DDoS- und Ransomware-Angriffen, festgestellt. Cyber-Kriminelle versuchen mit solchen Attacken, das Zielsystem mit einer großen Datenmenge derart zu überlasten, dass es für Nutzer nicht oder nur sehr eingeschränkt verfügbar ist.
7. Cyberkriminelle erfinden sich neu: Gestern Darkside heute Blackmatter, gerade noch Grandcrab, dann Revil: Steigt der Ermittlungsdruck auf eine Hackergruppe, löst sich diese häufig auf – nur um sich einige Zeit später unter einem anderen Namen neu zu erfinden. Häufig mit neuen Methoden und noch gefährlicher als vorher.
8. Emotet ist wieder da: Ransomware war zuletzt auch deshalb auf dem Vormarsch, weil der Trojaner Emotet, „die gefährlichste Software der Welt“, wieder auftauchte. Er dient als Türöffner, über den sich weitere Schad-Software nachladen lässt, auch Ransomware. Eigentlich wurde Emotet durch eine internationale Aktion im Januar 2021 zerschlagen, doch bereits im November tauchte er wieder auf.
9. Sicherheitslücke „Faktor Mensch“: Phishing zielt auf die Schwachstelle Mensch. Die Mitarbeitenden werden immer geschickter dazu verleitet, schädliche Anhänge zu öffnen und auf Web-Seiten mit Schadcodes zu gehen. Mitarbeiterschulungen sind kein geeignetes Mittel, um diese Angriffe abzuwehren. Auch ein Hinweis auf das Nicht-Öffnen von Anhängen ist ein völlig unzureichender Schutz vor Cyber-Angriffen. Denn der Mensch macht Fehler und solche Fehler können gravierende Folgen haben.
10. Gängige IT-Sicherheits-Tools sind machtlos: Angesichts dieses immer professionelleren und geschickteren Vorgehens der Täter reichen einzelne Firewalls oder Virenschutzprogramme längst nicht mehr aus.

Virtueller Browser bietet Schutz

Was können Unternehmen, Behörden und KRITIS also gegen diese steigende Gefahr tun? Der Browser ist das Einfallstor Nummer 1 für Ransomware und andere Schad-Ware. Der beste Schutz vor solchen Angriffen aus dem Internet ist ein virtueller Browser. Er erlaubt das Surfen im Internet, ohne dass Hacker Zugriff auf die Unternehmensnetzwerke erlangen können. Die Lösung R&S Browser in the Box von Rohde & Schwarz Cybersecurity etwa schließt die Sicherheitslücke Internet, indem sie eine digitale Quarantäne für Hacker-Angriffe ermöglicht. Auf der Rechnerebene erfolgt hier eine komplette Isolation, sodass Schad-Software vom restlichen PC des Nutzers ferngehalten wird. Zusätzlich wird auf der Netzwerkebene der Zugang zum Internet vom Intranet getrennt. Dieser Mechanismus schützt auch vor Angriffen via E-Mail-Anhängen oder bei Web-Konferenzen mit Mikrofonnutzung und Webcam-Unterstützung.
Kommt ein virtueller Browser zum Einsatz, haben Cyber-Kriminelle keine Chance. Darüber hinaus sollten weitere Schutzmaßnahmen vorgenommen werden – beispielsweise die Verschlüsselung der Endgeräte,

eine hochsichere VPN-Verbindung und die Absicherung des heimischen WLANs. Mit einem solchen 360-Grad-Schutz erschweren Behörden und KRITIS einen Angriff.

()

Weitere Informationen zum Schutz von KRITIS

Stichwörter: IT-Sicherheit, KRITIS, Ransomware, Rohde & Schwarz