Warum Ransomware immer gefährlicher wird

Hinter Cyber-Angriffen stecken in den meisten Fällen sogenannte Ransomware-Attacken – also Erpressungsangriffe, die Daten verschlüsseln oder abziehen und dann ein Lösegeld fordern. Die Zahl der Erpresserangriffe hat 2021 weiter zugenommen, so das BKA.

Der jährliche Schaden durch Ransomware ist in den vergangenen Jahren rasant gestiegen: auf ca. 24,3 Mrd. Euro in 2021 von 5,3 Mrd. Euro im Jahre 2019. Der durchschnittliche Schaden pro Attacke hat um 21 Prozent zugelegt. Der Ransomware-Trend ist nicht neu – doch die Gefährdungslage verschärft sich aktuell dramatisch.

10 Gründe für immer gefährlichere Ransomware

- 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 wachsen die Verbreitung und die Professionalisierung der Angriffe weiter an.
- 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 Schadsoftware – auch von Ransomware.
- Fake-E-Mails schüren die Angst. Phishing-E-Mails zum Thema Covid-19 haben 2021 zwar abgenommen. Doch Phishing-Nachrichten nehmen noch immer häufig auf aktuelle gesellschaftliche Entwicklungen Bezug, 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.
- 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 noch vor der Pandemie der Fall war.
- 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.
- DDoS verschärft Erpressungen. Zusätzlich zur Datenverschlüsselung und -veröffentlichung legen immer mehr DDoS (Distributed Denial of Service)-Attacken die Webseiten der Opfer lahm. Im Jahr 2021 hat das BKA verstärkt Multivektor-Angriffe, sog. Carpet-Bombing und eine Kombination von DDoS- und Ransomware-Angriffen, festgestellt. Cyberkriminelle versuchen mit solchen Attacken, das Zielsystem mit einer großen Datenmenge derart zu überlasten, dass es für Nutzer nicht oder nur sehr eingeschränkt verfügbar ist.
- 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.
- Emotet ist wieder da. Er dient als Türöffner, über den sich weitere Schadsoftware nachladen lässt, auch Ransomware. Eigentlich wurde Emotet durch eine internationale Aktion im Januar 2021 zerschlagen, doch bereits im November tauchte er wieder auf.
- Sicherheitslücke „Faktor Mensch". Phishing zielt auf die Schwachstelle „Mensch". Die Mitarbeitenden werden immer geschickter dazu verleitet, schädliche Anhänge zu öffnen und auf Webseiten 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 Cyberangriffen. .
- Gängige Sicherheits-Tools sind machtlos. Angesichts dieses immer professionelleren und geschickteren Vorgehens der Täter, reichen Firewalls oder Virenschutzprogramme nicht mehr aus.

Was können Unternehmen, Behörden und KRITIS dagegen tun?

Kommt ein virtueller Browser zum Einsatz, haben Cyberkriminelle 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.. ■

www.rohde-schwarz.com/sicherheit-fuer-kritis