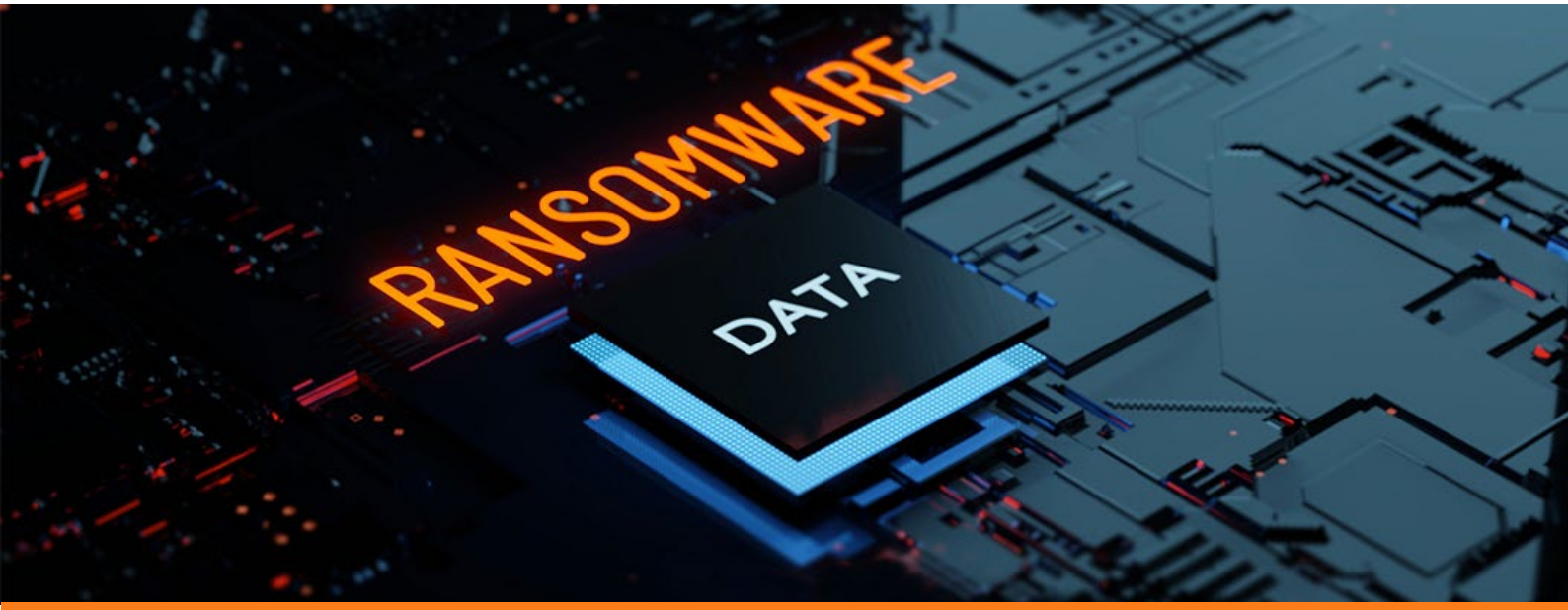


Whitepaper | IT Security

Ransomware auf dem Vormarsch

Wie gut sind Sie geschützt?

brandeins /thema 2022 Heft 22 Beste Unternehmensberater

Part of Consileon Group

Inhalt

Was ist Ransomware überhaupt? 3

Wie wird die Hardware infiziert? 4

Der Rechner ist infiziert: Wie geht es weiter? 4

Wie kann ich mich und mein Unternehmen schützen? 5

Die Gefahr steigt, die Sicherheitsmaßnahmen stagnieren 5

Neue Technologien bieten neue Angriffsflächen 6

Ihr Vorsprung mit syracom 7

Unser Angebot 7

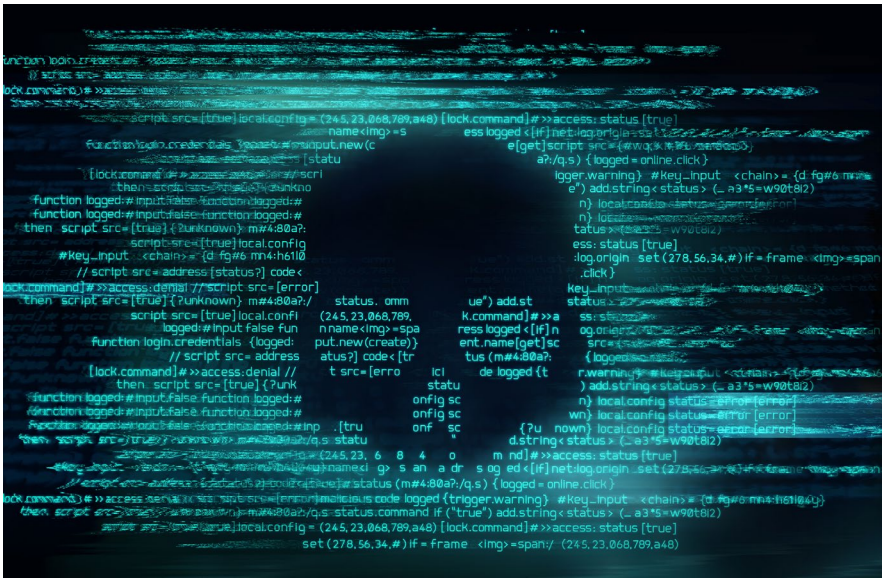
Referenzen 8

business efficiency engineering 9

Eine unbekannte Gruppe Hacker verschlüsselte vergangenen August dreißig Server des Düsseldorfer Uniklinikums. Durch den anhaltenden Ausfall der IT-Systeme wuchs die Anzahl der betroffenen Patienten von Tag zu Tag. Der Höhepunkt des Vorfalls war der Tod einer Patientin, die durch den Ausfall nicht rechtzeitig ins Krankenhaus gebracht werden konnte. Doch wieso haben Ransomware-Angriffe auf die IT-Infrastruktur mittlerweile eine so große Auswirkung?

Was ist Ransomware überhaupt?

Ransomware stellt, wie der Wortbestandteil „Ransom“ (zu Deutsch: Lösegeld) schon sagt, ein Loskaufen der Daten dar. Eine Erpressersoftware wird auf einzelne Rechner oder ganze Netzwerke geschleust. Dort verschafft sie sich schlimmstenfalls Zugriff auf die kompletten Daten, um diese zu verschlüsseln und unlesbar zu machen.



Anschließend folgen meistens Erpresserbriefe mit Lösegeldforderungen, die auf dem Bildschirm des digitalen Endgeräts erscheinen. Neben dem Verschlüsseln der Daten kann die Software auch einfach den Zugriff auf diese blockieren. Um die Kontrolle über das blockierte System zurückzuerlangen, hilft in manchen Fällen eine spezielle Antivirensoftware. Bei verschlüsselten Systemen sieht es hingegen anders aus: Um zeitnah wieder auf die Daten zugreifen zu können, muss meistens der Lösegeldforderung nachgegeben werden.

Wie wird die Hardware infiziert?

Oft passiert es schnell, unauffällig und nicht zurückverfolgbar: Der Computer oder Server wird über breit gestreute Phishing Mails, Websites oder den guten, alten USB-Stick infiziert. Eine weitere Möglichkeit ist das Einschleusen über technische Schwachstellen im Netzwerk oder einer Drittanbietersoftware. Im oben genannten Fall des Düsseldorfer Uniklinikums verschafften sich die Angreifer den Zugriff über eine Schwachstelle in einer weit verbreiteten kommerziellen Software.

Bevor sich die Ransomware ausbreiten kann, vergehen im Schnitt sieben Tage, bis der Eindringling zuschlägt. Sobald die Schadsoftware einen Weg in das System gefunden hat, beginnt sie je nach Absichten der Hacker die Arbeit an den Daten. Bei einer Software, die sich nicht um spezifische Daten kümmert, sondern so schnell und so viel wie möglich zerstören möchte, wird sofort mit der Verschlüsselung begonnen. Meist werden hierbei zuerst Daten attackiert, die als nicht systemkritisch eingestuft werden, sodass der Angriff nicht direkt bemerkt wird. Komplexere Ransomware kann sogar Abwehrmaßnahmen auf dem Rechner oder dem Netzwerk unterwandern und umgehen. Die Verschlüsselungsrate ist hier jedoch verlangsamt.

Der Rechner ist infiziert: Wie geht es weiter?

Wenn ein Device verschlüsselt oder blockiert wurde, ist die offensichtlichste Auswirkung, dass kein Zugriff mehr auf die Daten und Systeme besteht. Da eine Ransomware-Attacke meist ohne Vorlaufzeit durchgeführt werden kann, hat dies eine unmittelbar lähmende Wirkung. Je weiter die Infektion in einer IT-Infrastruktur vorangeschritten ist, umso schwerwiegender sind die Auswirkungen.

Die Betroffenen haben nach dem kompletten Ausfall des Systems kaum Möglichkeiten, der Attacke entgegenzuwirken. Bei aktueller Ransomware bleibt Unternehmen ohne Backup-Sicherungen meist nur das Zahlen des Lösegelds oder die Insolvenz.

Die Folgeschäden sind hier weit gestreut. Verschlüsselte Vertriebsdatenbanken, gesperrte Gehaltsabrechnungssysteme oder anderweitig gestörte Finanzsysteme: Wie viele Tage kann IHR Unternehmen so überleben? Deutlicher wird die Gefahr beim Betrachten von Systemen der kritischen Infrastruktur, wie zum Beispiel die Verfügbarkeit von Lebensmitteln, bei Stadtwerken oder Krankenhäusern.

Wie kann ich mich und mein Unternehmen schützen?

Ganz oben auf der Liste der Schutzmaßnahmen steht das regelmäßige Absichern der Systeme durch Backups auf externen Speichermedien. Für die Recovery-Maßnahmen sollten zudem alle Daten gesichert und entsprechende Backups überprüft werden. So gehen die Daten nicht verloren und können im Fall einer Verschlüsselung neu aufgespielt werden.

Eine Firewall, Antivirenprogramme, die sichere Konfiguration von Soft- und Hardware sowie fortlaufend Updates zu installieren, sind weitere wichtige Sicherheitsmaßnahmen. Zusätzlich kann über digitale Identitäten und das Need-to-know-Prinzip eine schnelle Ausbreitung der Ransomware gebremst werden.

Auch der Mensch spielt hier wieder als Risikofaktor eine große Rolle. Da die Ransomware meist über E-Mail-Anhänge, Fake-Webseiten oder den USB-Stick verteilt wird, hat der Nutzer hier selbst die Möglichkeit, als Firewall zu agieren und den Angreifern keine Chance zu geben.

Die Gefahr steigt, die Sicherheitsmaßnahmen stagnieren

Ransomware hat sich für die Angreifer zu einem sehr lukrativen Geschäft entwickelt, mit dem sie Geldbeträge in Millionenhöhe erpressen können. Kaum verwunderlich, dass im Jahr 2021 jedes dritte Unternehmen (37 Prozent) [1] betroffen war, Tendenz steigend.

Bei den Gegenmaßnahmen sieht der Ausblick hingegen düster aus. Auch wenn bereits einige Programme zum Entschlüsseln älterer Ransomware existieren, stellen diese nur einen Tropfen auf den heißen Stein dar.

Ein erster zaghafter Versuch der USA ist das Sanktionieren von unerlaubten Ransomware-Zahlungen. Dies ist möglicherweise auf lange Sicht effizient. Dennoch werden damit insbesondere die Unternehmen bestraft, die aktuell unter Beschuss erfolgreicher Attacken stehen. Die erschreckende Wahrheit ist: Außer dieser Maßnahme werden die Firmen weiterhin allein gelassen in der Hoffnung, dass sich das Problem von selbst erledigt. Zusätzlich stellt sich die Strafverfolgung als schwierig heraus. Angreifer können sich zum

Beispiel mithilfe von VPNs mittlerweile gut vor den Behörden verstecken. So können Hacker etwa suggerieren, sie befänden sich in Russland, während sie jedoch in China sitzen.

Fest steht: Das Thema Sicherheit in Bezug auf Ransomware stagniert.

Neue Technologien bieten neue Angriffsflächen

Mittlerweile beziehen die Angreifer weitere Technologien für Ransomware-Attacken ein. Smartphones stellen seit 2014 mitunter eine lukrative Möglichkeit für Cyberkriminelle dar. Dabei werden nicht nur die Daten verschlüsselt, sondern oft auch der Bildschirm gesperrt sowie das Passwort geändert. Der User kann damit nicht mehr auf sein Mobilgerät zugreifen. Durch die steigende Anzahl der Smartphones [2] und deren wachsende Bedeutung im Alltag sind hier in Zukunft mehr Angriffe zu erwarten.

Auch beim Internet der Dinge (kurz: IoT, Beispiel: Dash-Button von Amazon, Live-Paketverfolgung über das Internet) haben es Kriminelle mehr und mehr auf das Sperren des Geräts abgesehen – und die damit einhergehende Übernahme. Der Diebstahl oder das Verschlüsseln von Daten lohnt sich auf den einzelnen Maschinen hingegen kaum, da sich dort keine sensiblen Daten befinden. Bei einer hohen Anzahl von vernetzten Geräten im Unternehmen, die zu einem Botnetz zusammengefügt werden können, ist der Aufwand, diese zu hacken, nochmals höher.

Generell sind Ransomware-Attacken auf IoT-Hardware mit viel Aufwand für die Cyberkriminellen verbunden, der die Rentabilität enorm infrage stellt und gegen eine Attacke auf IoT-Hardware spricht.

Trotzdem sollten solche potenziellen Angriffe immer in Betracht gezogen werden – schließlich können die möglichen Auswirkungen mehr als erschreckend sein. So wäre es etwa denkbar, dass die Hacker Zugriff auf ein vernetztes Auto während der Fahrt erhalten. Ein weiteres Szenario wäre, dass ein Herzschrittmacher infiziert wird und plötzlich anfängt, Schläge zu überspringen [3]. Wer würde hier nicht die geforderten Bitcoins zahlen, wenn es um Leben und Tod geht?

Ihr Vorsprung mit syracom

syracom hat es sich gemeinsam mit ihren Partnern zur Aufgabe gemacht, einen themenübergreifenden und möglichst umfassenden Schutz gegen Ransomware bereitzustellen.

Unser Angebot

1. Wir helfen beim Aufbau eines Informationssicherheitsmanagementsystems zum Definieren, Steuern, Kontrollieren, Aufrechterhalten und Verbessern der Informationssicherheit.
2. Wir beraten Sie dabei, wie Sie Ihre Assets sichern, indem Sie Backups und Patches auf den Systemen durchführen und regelmäßig testen.
3. Wir führen für Sie reelle Angriffe hochautomatisiert und kosteneffizient durch, um zu prüfen, ob Ihre Prozesse, Systeme und Mitarbeiter wie gewünscht agieren.
4. Wir überprüfen und verbessern dauerhaft und konsequent Ihr Identity Management (IDM) für Mitarbeiter sowie Partner (kosteneffiziente Rechtevergabe des Unternehmens sollte im Mittelpunkt stehen).
5. Wir schulen Sie und Ihre Mitarbeiter in puncto Security Awareness (nachweislich einer der wichtigsten Bausteine im Kampf gegen Ransomware-Angriffe).

Entscheiden Sie sich jetzt dafür, wirksame Schutzmaßnahmen zu implementieren und Schadenspotenzial zu verringern. Unsere Berater sind gerne für Sie da und erstellen für Sie ein themenübergreifendes und individuelles Angebot.

Referenzen

[1] Weitere interessante Zahlen sind dem Report „Status quo von Ransomware 2021“ des britischen IT-Security-Anbieters Sophos zu entnehmen

[2] Aktuelle Lage der Smartphone-Entwicklung https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der- smartphonenutzer-in-deutschland-seit-2010/

[3] https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/

- “We wait, because we know you.” Inside the ransomware negotiation economics. – NCC Group Research

- BSI – Ransomware – Vorsicht vor Erpressersoftware (bund.de)

- endpoint-survey-report.pdf (sophos.com)

- The Ransomware Files (google.com)

business efficiency engineering
für exzellente Geschäftsprozesse

syracom ist ein unabhängiges Business- und IT-Beratungshaus, spezialisiert auf die Gestaltung effizienter und nachhaltiger Geschäftsprozesse.

Seit der Gründung im Jahr 1998 unterstützt syracom ihre Kunden dabei, Business- und IT-Strategien in flexible und wettbewerbsfähige Lösungen für große und mittelständische Kunden unterschiedlicher Branchen umzusetzen.

Unsere Experten begleiten den Kunden bei der digitalen Transformation seiner Geschäftsprozesse entlang der Wertschöpfungskette: von der Planung über die Steuerung und Optimierung bis zur Umsetzung.

Dr. Philip Tauschek
Geschäftsführender Partner

Marius Dreixler
IT Security Consultant

syracom AG
Otto-von-Guericke-Ring 15
65205 Wiesbaden (Germany)

philip.tauschek@syracom.de
Fon: +49 6122 91760
www.syracom.de