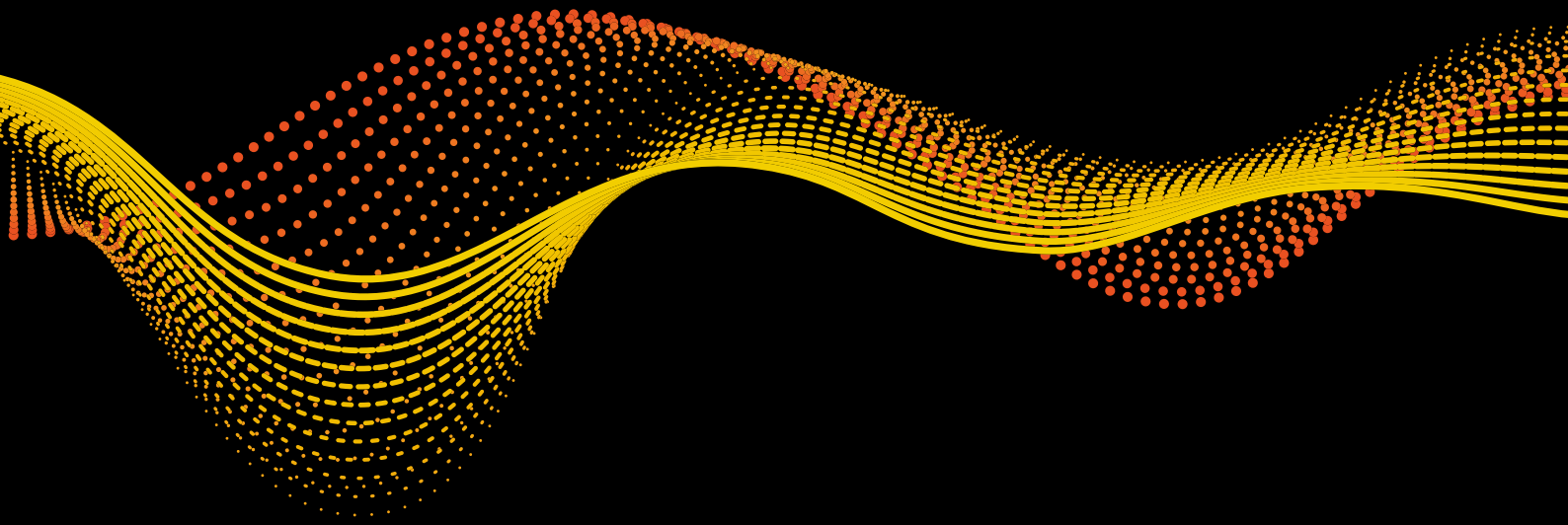
2|22
Auszug aus
Ausgabe 2
April 2022

e|m|w

Das ener|gate-Magazin.



Schwerpunkt Safer EVU

Ransomware die Angriffsfläche nehmen

Von **Michael Haas**, Regional Vice President Central Europe, Watchguard Technologies

ISSN: 1611-2997

Foto: © imaginima/istockphoto

Ransomware die Angriffsfläche nehmen

Der Erpresser von heute droht Menschen und Einrichtungen nicht mehr mit physischen Schäden, sondern dringt in die IT-Systeme von Unternehmen ein, um deren Daten zu verschlüsseln. Ransomware gehört zu den modernen Geißeln der IT-Security-Welt und die erfolgreiche Abwehr digitaler Angriffe verlangt Unternehmen Maßnahmen auf unterschiedlichsten Ebenen der internen Sicherheitsstrategie ab.

Von **Michael Haas**, Regional Vice President Central Europe, Watchguard Technologies

Die Geschichte von Erpressungssoftware reicht etwa 40 Jahre zurück. Bereits in den 1980er Jahren attackierte ein britischer Arzt AIDS-Forscher Computer per Diskette mit einem Bootloader-Virus, das Computer sperrte. Damals wurden die Opfer noch aufgefordert, Bargeld per Post zu übermitteln. Spätestens mit dem Aufkommen von Cryptolockern – die aufgrund der breiten Streuung als Schrotflinten-Ransomware bezeichnet werden – und dem Trend zu Ransomware-as-a-Service hat die einschlägige Gefahr seit einigen Jahren jedoch ganz neue Dimensionen erreicht.

Nicht nur der Branchenverband der deutschen Informations- und Telekommunikationsbranche Bitkom e.V. verzeichnet in dem Zusammenhang eine klare Zunahme entsprechender Angriffe, die es mit Sorge zu betrachten gilt. Denn mittlerweile brechen Angreifer in Netzwerke ein und wenden viel Zeit dafür auf, die Opfer im Detail auszukundschaften. Ziel ist es, Ransomware auf so vielen Geräten wie möglich zu platzieren, um auf diese Weise von jetzt auf gleich für umfassende Verschlüsselung zu sorgen.

Dass die Folgen verheerend und kostspielig sein können, hat unter anderem der Fall der Colonial Pipeline in den USA gezeigt. Aber auch deutsche Unternehmen sind vor der spezifischen Bedrohung nicht gefeit. Neben einem auf den Energiemarkt ausgerichteten Softwareanbieter waren hierzulande in jüngster Vergangenheit etliche Energieversorger selbst betroffen.

In der Regel begnügen sich Cyberkriminelle dabei nicht mehr nur mit der „klassischen" Erpressung, bei der verschlüsselte Daten nach Lösegeldzahlung wieder freigegeben werden. Stattdessen werden weitere Wertschöpfungsstufen verfolgt. Immer häufiger kommt es auch zum Diebstahl unternehmensinterner, sensibler Daten unter Androhung von Veröffentlichung, sollte nicht gezahlt werden. Im schlimmsten Fall sind sogar Partner- und Kundendaten betroffen oder DDoS-Attacken inkludiert.

» Angreifer verwenden oft gestohlene oder durchgesickerte Anmeldedaten, die sie per Phishing-E-Mail abgegriffen oder im Dark Web gefunden haben.

Wie perfide sich solche Angriffe inzwischen gestalten, demonstriert ein Beispiel aus Finnland aus dem Jahr 2020: Nachdem die betroffene Gesundheitsorganisation, der Hacker vertrauliche Psychotherapiedaten von 40.000 Patienten entwendet hatten und mit deren Bekanntmachung drohten, kein Geld zahlte, richteten die Kriminellen ihre Lösegeldforderung ganz einfach an die betroffenen Patienten selbst.

Die mit Ransomware einhergehenden Risiken sind also offensichtlich. Dennoch scheitern gerade mittelständische Unternehmen nach wie vor nicht selten daran, adäquate Verteidigungslinien zu ziehen, die auf unterschiedlichen Ebenen Wirksamkeit entfalten. Dass von E-Mails immanente Gefahr ausgeht, wissen die meisten. Doch darüber hinaus gibt es zahlreiche andere Angriffsvektoren und vielfältige Ablaufmuster im Zuge von Ransomware-Attacken. Im Folgenden soll daher der Fokus auf die wichtigsten Elemente einer zielführenden Abwehrstrategie gerichtet werden.

Regelmäßiges Patchen

Der erste Schritt zu mehr Sicherheit erscheint zunächst einfach: Patchen. Die Aktualisierung der Unternehmenssoftware – insbesondere bei öffentlich zugänglichen Ressourcen wie Webanwendungen oder Webservern – ist von entscheidender Bedeutung. Schließlich sind Angreifer über solch offene Flanken in der Lage, Malware ohne jegliches Zutun auf Anwenderseite in die Organisation einzuschleusen. Dafür nutzen sie meist nur alte Schwachstellen aus (Zero-Day-Lücken sind relativ selten), für die es zum Teil schon längst einen Patch gibt. Gerade für Administratoren von Unternehmen mit hybriden IT-Strukturen, die klare Anforderungen hinsichtlich der Verfügbarkeit erfüllen müssen, wird ein konsequentes Patchen jedoch schnell zur Herausforderung.

Strenge Passwortrichtlinien

Ein weiterer Punkt sind sichere Passwörter. Die alte IT-Security-Weisheit „Hacker brechen nicht ein, sie loggen sich ein" bewahrheitet sich immer wieder. In den meisten Fällen verwenden Angreifer gestohlene oder durchgesickerte Anmeldedaten, die sie per einfacher Phishing-E-Mail abgegriffen oder im Dark Web gefunden haben. Auf diese Weise steht dem Cyberbösewicht die Tür ins Unternehmensnetzwerk jederzeit und ohne Mühe offen.

Ist die initiale Hürde erstmal überwunden, kann er mit speziellen Tricks und Werkzeugen seine Zugriffs- und Handlungsmöglichkeiten massiv ausweiten. Kennwörter sollten daher strengen Vorgaben genügen. Da sich die meisten Menschen eine Vielzahl von Login-Informationen merken müssen, ist der Einsatz eines Passwort-Managers sinnvoll. Dieser ermöglicht es dem Nutzer, über ein komplexes Passwort oder eine komplexe Phrase den Zugriff auf andere Zugangsdaten abzusichern. So können sogar 32-stellige Zufallspasswörter verwendet werden, ohne dass man sich diese alle einzeln merken muss.

Einführung einer Multifaktor-Authentifizierung

An das Thema Passwörter schließt sich ein weiteres Element zur Abwehr unerwünschter Eindringlinge nahtlos an: Multifaktor-Authentifizierung. Denn nur damit lassen sich Passwörter und dahinterstehende Benutzeridentitäten wirklich nachhaltig absichern. Das Prinzip dabei ist es, mehrere Methoden der Authentifizierung zu kombinieren, um auf diese Weise für zusätzlichen Schutz zu sorgen. Bei der Einwahl via Username und Passwort zählt allein das Wissen. Deshalb gilt es, darüber hinaus Faktoren wie „Besitz" und „Biometrie" einzubinden.

Besonders anwenderfreundlich ist in diesem Fall die Integration von Smartphones. Nach der gewohnten Eingabe der Login-Daten erhält der Anwender eine Push-Benachrichtigung auf sein – vom Administrator eindeutig zugeordnetes – Telefon, das er mit Face-ID entsperren muss, um die Zugriffsanfrage zusätzlich zu bestätigen. Ein Hacker, der zwar das Passwort kennt, aber nicht im Besitz der weiteren Bestätigungsinstanz ist, hat hier das Nachsehen. Die Spielarten der Mehrfaktor-Authentifizierung sind dabei durchaus vielfältig.

Auch andere Hardwarekomponenten wie Smart Cards oder USB-Token – welche eine stetig wechselnde und zeitlich begrenzt gültige Zahlenkombination nach dem OTP-Verfahren (One Time Password) anzeigen – sowie zusätzliche Softwarepakete oder die Authentifizierung via E-Mail, PIN oder Sicherheitsfrage sind in der Praxis üblich und gewährleisten ein Plus an Sicherheit.

Back-ups als doppelter Boden

Bei Ransomware-Attacken sind Back-ups ebenfalls von entscheidendem Wert – zumindest, wenn es der Erpresser allein auf die Datenverschlüsselung abgesehen hat. „Gekaperte" Daten lassen sich damit auch ohne Lösegeldeinsatz einfach wiederherstellen – Disaster Recovery ist in jeder Form möglich, ganz unabhängig von der Ursache. Im Rahmen von Ransomware-Abwehrstrategien zählen jedoch die Details. Denn natürlich wissen Angreifer, dass Back-ups ihren Zielen entgegenstehen und sind bestrebt, solche Sicherungsdienste rechtzeitig auszuschalten. Daher sollten Unternehmen der 3-2-2-Regel folgen, was bedeutet, dass mehrere Kopien an verschiedenen Stellen intern und gleichzeitig extern physisch sowie in einer Cloud bestmöglich abgeschirmt hinterlegt werden.

> Für effektiven Schutz sind Algorithmen des maschinellen Lernens und erweiterte Möglichkeiten der Verhaltenserkennung nötig.

Fortschrittlicher Malware-Schutz

Eine weitere Stellschraube im Kampf gegen Ransomware ist ein moderner Malware-Schutz. In den vergangenen Jahrzehnten basierte die Malware-Erkennung und -Prävention in erster Linie auf Signaturen – oder war auf bekannte Muster und spezifische Dateien ausgerichtet. Dieser Ansatz ist jedoch rein reaktiv. Wenn ein Angreifer eine neue Malware veröffentlicht – sagen wir, es handelt sich um Ransomware – muss ein Experte oder ein automatisiertes Sicherheitsforschungsprogramm die Datei erst einmal gefunden und als schädlich eingestuft haben, bevor ein solches Programm zur Mustererkennung Wirkung entfalten kann.

Leider agiert Malware von heute sehr ausweichend und polymorph (WannaCry kommt beispielsweise in tausenden Versionen daher). Untersuchungen wie der Internet Security Report von Watchguard zeigen, dass sich ein Löwenanteil der Malware mittlerweile dem Radar einer signaturbasierten Erkennung entzieht. Für effektiven Schutz vor (Zero-Day-)Malware – zu der auch ausweichende Ransomware oder die Stager gehören, die zur Verbreitung von Ransomware verwendet werden – sind daher Algorithmen des maschinellen Lernens und erweiterte Möglichkeiten der Verhaltenserkennung nötig.

Absicherung von Endpoints

Der Einsatz von EDR-Funktionalität (Endpoint Detection and Response) ist ein ebenso wichtiges Puzzleteil. Neue Angriffe nach dem „Living off the land"-Prinzip nutzen legitime Teilbereiche eines Betriebssystems (zum Beispiel in Windows PowerShell) gezielt aus. Das Einschleusen von Malware in „autorisierte" Prozesse – ohne die Schadware als Datei auf dem Computer selbst zu speichern – lässt sich nur abwenden, wenn sowohl der Speicher als auch alle laufenden Prozesse überwacht und im Hinblick auf DLL- oder Prozessinjektion gescannt werden. EDR-Lösungen untersuchen die Aktivitäten nach der Ausführung und helfen, Anomalien aufzuspüren. Somit tragen sie nachhaltig zur Vorbeugung einschlägiger Angriffe bei.

Sensibilisierung der Anwender

Last but not least dürfen Schulungen im Werkzeugkasten der Ransomware-Abwehr nicht fehlen. Unternehmen müssen sicherstellen, dass jeder einzelne Mitarbeiter die Grundlagen der E-Mail-Sicherheit beherrscht und weiß, was beispielsweise Spear Phishing ist und wie man es erkennt. Die Sensibilisierung sollte dabei von der Umsetzung eines gezielten Berechtigungsmanagements begleitet werden. Denn was hilft es, wenn ein Netzwerk nach außen wie Fort Knox daherkommt, für jeden darin aber maximale Freiheit gilt. Insofern kommt es darauf an, Zugriffsrechte einzelner sinnvoll einzuschränken und zu überwachen. Ein Buchhalter benötigt schließlich keinen Zugang zu einer technischen Datenbank.

Fazit

Unternehmen, die all diese Aspekte ins Kalkül ziehen und auf mehrschichtige Sicherheit bauen, sind in Sachen Ransomware-Schutz klar im Vorteil. Damit die Komplexität nicht ins Unermessliche steigt, sollte zudem, wo immer möglich, auf Konsolidierung der zugrundeliegenden Lösungsbausteine und zentrale Administrationsmöglichkeiten geachtet werden. Auch ein Outsourcing an professionelle Partner in Form von Managed Services kann dazu beitragen, die Verteidigung nachhaltig zu stärken, wobei gleichzeitig eine schwere Last von den Schultern der eigenen Mitarbeiter genommen wird.

MICHAEL HAAS

Jahrgang 1965

→ 1987–1991 Studium der Elektrotechnik, Fachhochschule Gießen-Friedberg

→ ab 2002 Territory Account Manager DACH, WatchGuard Technologies

→ seit 2020 Regional Vice President Central Europe bei WatchGuard Technologies

michael.haas@watchguard.com

e|m|w

Das ener|gate-Magazin.

energate gmbh

Norbertstraße 3–5
D-45131 Essen

Tel.: +49 (0) 201.1022.500
Fax: +49 (0) 201.1022.555

www.energate.de