Ich seh' etwas, was du nicht siehst

Und das ist (noch) unbekannt

Digitalisierung ist ein Thema, das uns alle derzeit betrifft. Viele Firmen haben in neue Arbeitsstrukturen investiert und diese Tendenz steigt weiterhin. So werden neue Möglichkeiten des digitalen Abreitens erschlossen, die mehr Flexibilität und Produktivität ermöglichen. Doch schwerwiegende Ereignisse im Bereich der Cyberkriminalität Anfang des Jahres haben gezeigt, dass Unternehmen hier auch Gefahren ausgesetzt sind. Wie Sie sich gegen noch unbekannte Gefahren schützen können.

Im Dezember 2020 erreichte die IT-Welt eine Nachricht über eine Schwachstellenkombination in Exchange Servern, die eine Übernahme des Servers erlaubte. Ausgeführt wurden die Angriffe von einer als Hafnium bekannt gewordenen Gruppe, die von China aus operierte und Informationen aus verschiedenen Industriezweigen abgegriffen hat. Mitte Januar 2021 wurden dann erste Presseberichte im breiteren Medienspektrum veröffentlicht. Doch außerhalb des Fachpublikums gab es wenig Wissen um diesen Angriff. Währenddessen waren primär amerikanische Firmen Ziel der Angriffe, und es wurden enorme Datenmengen erbeutet.

Diese Ereignisse führten Microsoft Anfang März 2021 zu einer Mitteilung. Auch wenn Ursachen und Vorgehensweise größtenteils bekannt waren, gab es noch keinen wirksamen Schutz. Patches mit effektiver Wirkung wurden erst Mitte März voll zugänglich gemacht.

Ein Täter kommt selten allein

Wie immer bei erfolgreichen Aktionen gibt und gab es Trittbrettfahrer. So kam es zu weiteren Operationen innerhalb der Cyberkriminalität. Hafnium betrieb Datenraub, doch die Trittbrettfahrer hatten anderes im Sinn. Die Operation „Black Kingdom" beispielsweise verlegte sich auf Verschlüsselungserpressung. Das Einfallstor: Der von Hafnium genutzte Angriff.

Und um die Zeitlinie abzuschließen: Mitte April 2021 kam eine Erinnerung und dringender Hinweis von Microsoft, die Sicherheitspatches auf Exchange Servern zu installieren. Auch wenn Microsoft schnell reagiert und sich der schweren Aufgabe angenommen hat, hier wieder für Sicherheit zu sorgen. Die Datenlücken waren gravierend. Wie kann man sich davor schützen?

Ein gefährliches Spiel

Genau hier trifft unser Kinderspiel. Wenn ich mehr sehe als jeder andere, gewinne ich das Spiel – das Spiel um die Sicherheit Ihrer Systeme.

Ein Weg diesem Angriff auf Exchange Servern zu begegnen, gelang mithilfe eines SIEM-Systems, das eine Echtzeitanalyse unter Einbeziehung unterschiedlicher Bedrohungsinformationen ermöglicht. So konnten auffällige Kombinationen von normalen Servervorgängen sichtbar gemacht werden. Die Überprüfung solcher Kombinationen zeigt dann Schwachstellen im Sicherheitssystem auf. Und am Ende kann so der Abfluss von Daten oder die Verschlüsselung der Daten zwecks Erpressung verhindert werden.

Die sichere Abwehr

Die konsequente Beobachtung von Servern und der ausgeführten Vorgänge generiert hierbei ein Muster, das als normal eingestuft wird. Durch einfache Farbkodierung können normale und neue Vorgänge unterschieden werden. Dies fügt dem Köcher der IT Security einen weiteren Pfeil zur Abwehr hinzu. Und wer hat das nicht gerne? Noch bevor große Anbieter mühsam einen neuen Sicherheitspatch programmiert haben, ist man in der Lage den Angriff zu erkennen. Die Firewall wird dann entsprechend konfiguriert, oder mit Serverrichtlinien die Ausführung der suspekten Vorgänge unterbunden.

Wer mehr sieht, der weiß mehr. Auch über unbekannte Angreifer und Angriffe. ■

Zu den Personen

Rolf Ramacher ist Geschäftsführer des Unternehmens SPRINTER Software. SPRINTER Software ist auf die Digitalisierung von Geschäftsprozessen spezialisiert und bietet individuelle Lösungen für Unternehmen an.
www.sprinter-software.de

Florian Eppinger ist Geschäftsführer von Eppinger Engineering Solutions GmbH (EES). Sein Unternehmen vereinigt mehr als 60 Jahre praktische Erfahrung im Bereich von Produktentwicklung, Innovationsprozessen und CRM Projekten.
www.ees-engineering.de