Advertorial

SWS COMPUTERSYSTEME

Eine kleine Sicherheitslücke im Firmennetzwerk reicht Hackern, um den ganzen Betrieb lahmzulegen.
Foto: Maksim Kabakou - stock.adobe.com

Schwachstellen im Check

Seit Beginn der Pandemie ist die Zahl von Cyberangriffen sprunghaft angestiegen. Unternehmen müssen deshalb in Sicherheitsmechanismen investieren.

Von Jonas Raab

REGENSBURG. Die digitale Transformation nimmt seit der Coronakrise in nahezu allen Branchen Fahrt auf, doch die IT-Sicherheit bleibt dabei oft auf der Strecke. Die zahlreichen Hackerangriffe auf ostbayerische Unternehmen in den vergangenen Monaten lassen bei Cyber-Security-Spezialisten wie Hans-Martin Kuhn die Alarmglocken schrillen.

Kuhn ist IT-Securityexperte bei SWS Computersysteme und bekommt es in regelmäßigen Abständen mit gefährlichen IT-Schwachstellen von Unternehmen aller Art zu tun. Zusammen mit der IT-Security-Kommandozentrale des Regensburger Systemhauses, dem Security-Operation-Center (SOC), deckt er im Kundenauftrag Anomalien und Sicherheitslücken über spezielle Schwachstellenscans auf. „Wir nutzen dafür die gleichen Werkzeuge und Verfahren wie die Hacker“, erklärt Kuhn. In den vergangenen Monaten hatten Kuhn und sein SOC alle Hände voll zu tun.

Hacker nutzen Corona aus

Dass Cyberangriffe seit Beginn der Pandemie – auch in der Region – sprunghaft angestiegen sind, bemerken nicht nur die IT-Experten bei SWS: Mitte April legte NTT Ltd., ein weltweit agierender Technologiedienstleister, den Global Threat Intelligence Report 2021 (GTIR) vor. Der Bericht macht deutlich, wie gezielt Hacker die derzeitige Ausnahmesituation ausnutzen, indem sie wichtige Branchen und gängige Schwachstellen aus der Umstellung auf Remotearbeit ins Visier nehmen: In der Fertigungsindustrie kam es 2020 zu 300 Prozent mehr Cyberangriffen als im Vorjahr, im Gesundheitswesen betrug die Zunahme 200 Prozent und in der Finanzbranche 53 Prozent. Laut Securityspezialist Kuhn müssten sich IT-Abteilungen in Unternehmen deshalb in regelmäßigen Abständen eine Reihe von Fragen stellen: Wie werden Netzwerke verwaltet und gesteuert? Wie werden sie segmentiert? Wie steht es um das Schwachstellenmanagement? Wie sind die Verantwortlichkeiten bei Sicherheitsereignissen verteilt, wie die Meldewege festgelegt? Das sei aber längst nicht alles, erklärt Kuhn: „Das Feld ist riesig.“

Unterstützung finden Unternehmen aller Branchen im Security-Operation-Center von SWS. Hier werden alle Sicherheitsmaßnahmen für die Kunden gesteuert. Dabei setzt SWS unter anderem auf Netzwerk- und Logdatenanalysen. Auf diese Weise lassen sich mögliche Angriffe früh aufdecken und nachverfolgen.

Bei den meisten Angriffen handelt es sich um Phishingangriffe – welche oftmals Ransomware-Attacken nach sich ziehen – oder auch um Exploits gegen ungepatchte Systeme. Bei sogenannten Zero-Day-Exploits handelt es sich um Sicherheitslücken, die den Softwareanbietern noch nicht bekannt sind und für die somit keine Patches zur Verfügung stehen. „Die Angreifer kommunizieren solche Schwachstellen im Darknet. Das wird in Zukunft immer häufiger der Fall sein“, so die SWS-SOC-Analysten Patrick Reichenberger und Korbinian Simonis. Als Unternehmen müsse man deshalb unbedingt über entsprechende Sicherheitsmechanismen verfügen, erklärt Kuhn. „Eine hundertprozentige Sicherheit gibt es natürlich nie, aber wir können die Angriffsfläche auf ein Minimum reduzieren.“

Der ganzheitliche Ansatz von SWS unter Einsatz eines SIEM (Security Information & Event Management) soll die IT-Sicherheit eines Kunden dauerhaft gewährleisten. Ein SIEM ist eine Plattform, über die sich Logdaten aller Endgeräte, Server, Netzwerkkomponenten, Anwendungen und Datenbanken auf sicherheitskritische Ereignisse und Auffälligkeiten hin überwachen lassen.

Da immer mehr Unternehmen ihren Mitarbeitern für die Arbeit aus dem Homeoffice einen Remotezugriff etwa durch die Verwendung von Client-Portalen anbieten, sind webapplikations- und anwendungsspezifische Angriffe sprunghaft angestiegen. Microsofts Exchange-Software ist das prominenteste Opfer solcher Angriffe, aber lange nicht das einzige: 67 Prozent aller Vorfälle im vergangenen Jahr entfielen laut GTIR auf diese Art von Cyberattacken. Damit haben sie sich in den letzten zwei Jahren mehr als verdoppelt.

Die „menschliche Firewall“

Die stark gestiegene Gefahr aus dem Cyberraum unterschätzen aktuell noch viele Unternehmen. „Bei manchen Firmen ist die Wahrnehmung nicht sehr ausgeprägt “, sagt Kuhn und berichtet von zahlreichen Fällen, in denen betroffenen Unternehmen gar nicht klar war, in welch heikle Situation sie gerade geraten sind. „Wenn personenbezogene Daten zum Angriffsziel werden, liegt eine Datenschutzverletzung vor. Der Vorfall muss dann innerhalb von 72 Stunden dem Landesamt für Sicherheit in der Informationstechnik (LSI) gemeldet werden, sonst begeht man eine Rechtsverletzung“, erklärt er.

Ein gesteigertes Bewusstsein für IT-Sicherheit ist laut Hans-Martin Kuhn genauso wichtig wie die technische Komponente. Er nennt das „menschliche Firewall“. Für den Umgang mit Bedrohungen bietet SWS deshalb Awareness-Kampagnen an. Schulungen und sogar simulierte Phishingaktionen sollen die Mitarbeiter der SWS-Kunden sensibilisieren und ein Bewusstsein für die Bedeutung der IT-Sicherheit schaffen.

Daten sind kostbare Schätze des digitalen Zeitalters

Datenschutz ist heute wichtiger denn je. Um ihn zu gewährleisten, setzen Experten auf verschiedene Methoden und Werkzeuge.

Von Jonas Raab

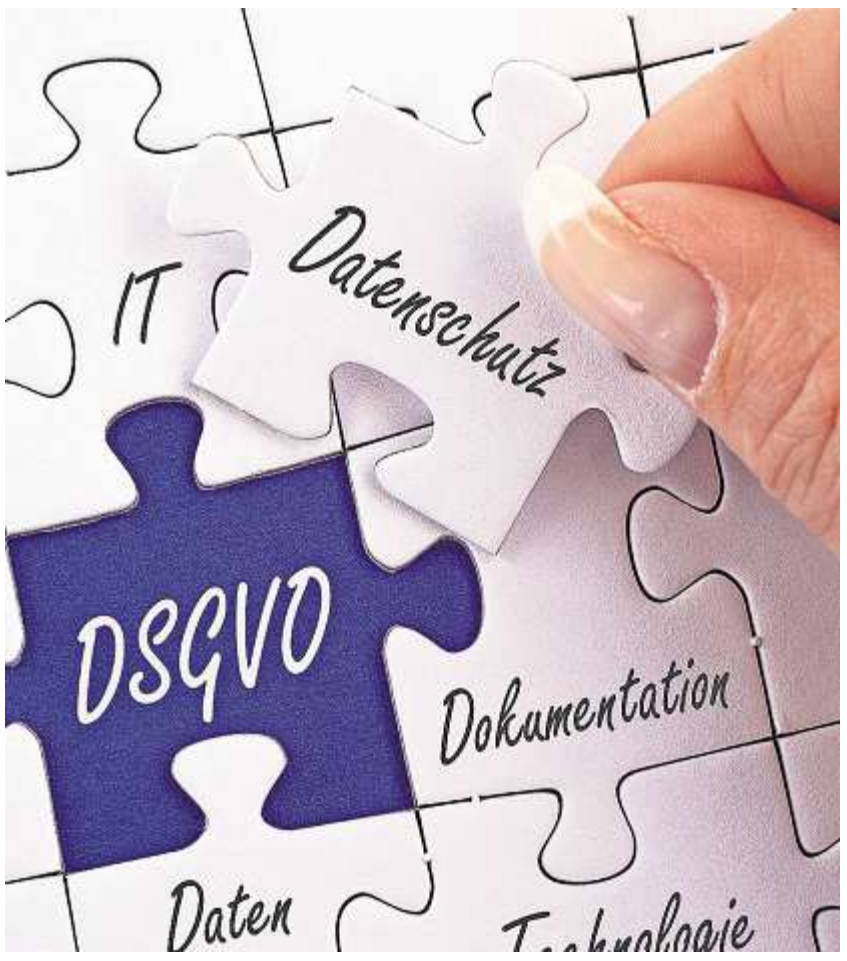
REGENSBURG. Nehmen Cyberkriminelle ein Unternehmen ins Visier, zielt ihr Fadenkreuz meist auf Daten. Sie sind die kostbaren Schätze des digitalen Zeitalters und bedürfen deshalb eines besonderen Schutzes. „Es muss sich dabei auch nicht gleich um Hackerangriffe handeln, es kann auch intern zu Datenabfluss kommen“, sagt Hans-Martin Kuhn, IT-Securityexperte bei SWS Computersysteme.

Um Daten zu schützen, gibt es verschiedene Methoden und Werkzeuge. Dabei gehe es gar nicht nur um IT-Security, sondern auch um Aufbewahrungsfristen oder gesetzliche Rahmenbedingungen. „Interne Prozesse und Arbeitsabläufe müssen gemäß den aktuell gültigen Datenschutzbestimmungen ablaufen und einer regelmäßigen Qualitätsprüfung unterzogen werden“, erklärt Kuhn.

Der erste Schritt: Die Daten eines Unternehmens müssen kategorisiert werden, besonders schützenswerte Akten wie Personal- oder Entwicklungsdaten dabei identifiziert werden. Anschließend gilt es, eine Berechtigungsmatrix zu erstellen. „Das ist in erster Linie eine organisatorische Frage. Bei vielen Unternehmen ist da allerdings noch viel Luft nach oben“, sagt Kuhn. In seiner täglichen Arbeit für die IT-Sicherheit seiner Kunden deckt er solche Fälle auf. Ein einfaches und alles andere als seltenes Beispiel: Ein Mitarbeiter verlässt ein Unternehmen, kann aber auf Wochen, Monate oder gar Jahre noch auf E-Mails oder den Firmenserver zugreifen. „Wahrnehmung und Realität klaffen in Unternehmen oft auseinander“, berichtet Kuhn. Um solche Fälle überhaupt aufzudecken, bietet SWS Computersysteme sogenannte Assessments an. Dabei erörtern die IT-Spezialisten den Istzustand bei ihren Kunden, geben ihnen Empfehlungen an die Hand und weisen sie gegebenenfalls auf offenstehende Einfallstore für Cyberkriminelle hin.

„Wir stellen dazu auch entsprechende Sicherungsmechanismen zur Verfügung, beispielsweise Werkzeuge zur Data-Loss-Prevention und für das Berechtigungsmanagement“, sagt Kuhn. Damit lassen sich alle Zugriffe auf Daten eines Unternehmens nachverfolgen.

Wie die IT-Sicherheit an sich, geht Datenschutz weit über Platinen, Rechner und Netzwerke hinaus. „Da geht es auch im 21. Jahrhundert noch um physische Sicherheit“, sagt Kuhn und meint damit Zugangsberechtigungen, Notizen oder anderweitige Informationen, die überall herumliegen können. SWS Computersysteme bietet neben seinen IT-Dienstleistungen deshalb auch Begehungen vor Ort an und analysiert die physische Datensicherheit, beispielsweise des Serverraums, seiner Kunden.



Datenschutz und Informationssicherheit sind ein weites Feld. Für Unternehmen gibt es einiges zu beachten. Foto: DOC RABE Media - stock.adobe.com

KONTAKT

SWS Computersysteme AG
Im Gewerbepark D 75
93059 Regensburg
Telefon: +49 (0) 941 / 20605-0
info@sws.de
www.sws.de

SWS COMPUTERSYSTEME
Member of ACP Group