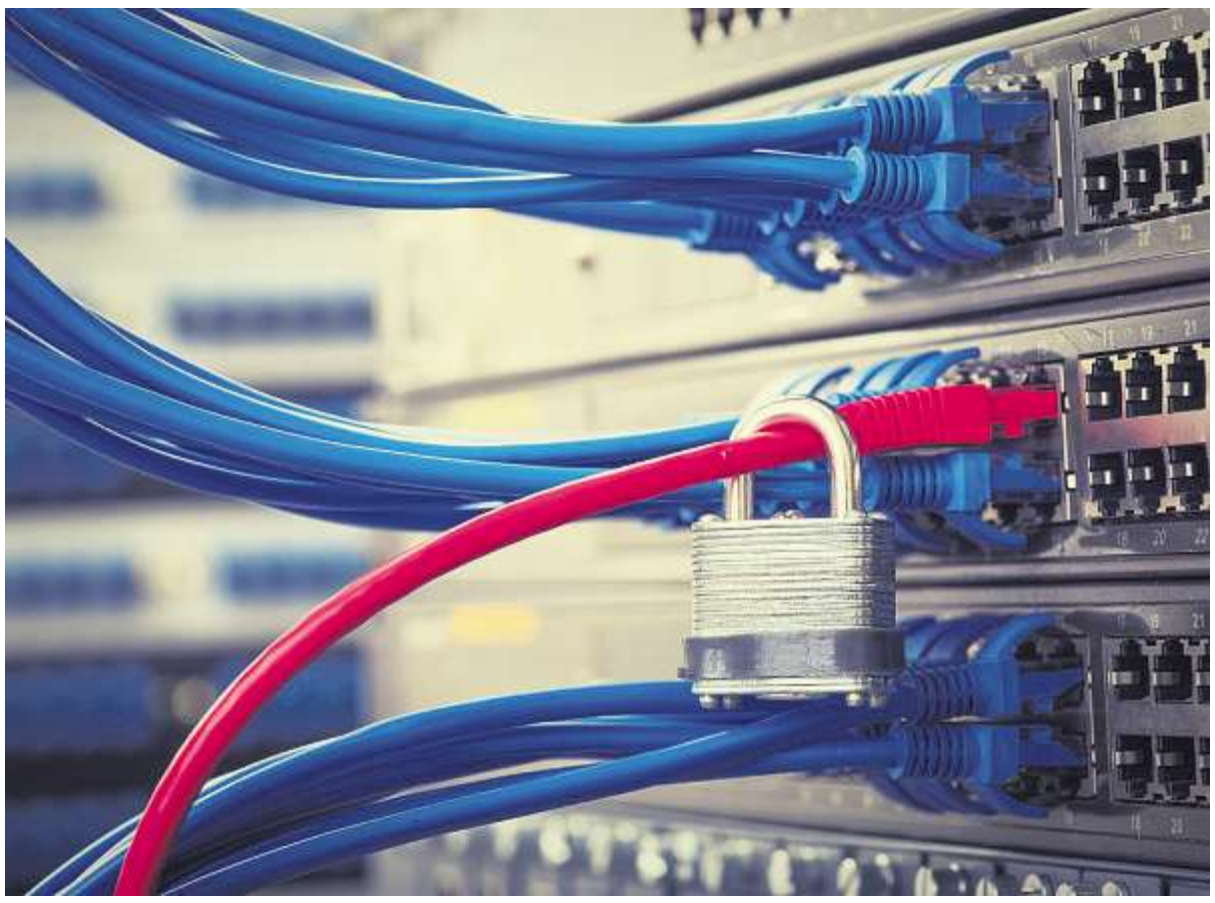
Advertorial

SWS COMPUTERSYSTEME



Netzwerke sind vielen externen und internen Gefahren ausgesetzt. Foto: xiaoliangge - stock.adobe.com

IT-Sicherheit muss mitwachsen

Neue Angriffsarten und der „Faktor Mensch“ stellen die IT-Sicherheit immer wieder auf den Prüfstand. Für ganzheitlichen Schutz sorgt die SWS Computersysteme AG.

Von Stephanie Burger

REGENSBURG. Cyberattacken gehören zum Unternehmensalltag – auch in kleinen und mittleren Unternehmen (KMU): Laut einer Studie des Netzwerkausrüsters Cisco mit 1816 IT-Verantwortlichen aus 26 Ländern erlitt mehr als die Hälfte der KMU 2018 eine Datenpanne. Die größten Sorgen bereiten Phishing, also betrügerische Angriffe auf Mitarbeiter, neue Arten von Schadsoftware und Denial-of-Service (DoS)-Attacken, die die Server eines Unternehmens mit so viel Traffic überfluten, dass sie kollabieren. Ebenfalls alarmierend: 40 Prozent der befragten Untnernehmen waren acht Stunden oder länger aufgrund eines größeren Sicherheitsverstoßes offline.

„Die Qualität der Angriffe nimmt zu, es gibt immer mehr Angriffsflächen und nach wie vor fehlt es an IT-Sicherheits-Bewusstsein“, sagt Zoran Andrijevic – Head of IT der SWS Computersysteme AG. Er schildert ein Angriffsszenario, das vor Kurzem Aufsehen erregte: Hacker hatten über Mitarbeiter manipulierte, mit einem WLAN-Empfänger versehene Ladekabel in Firmen eingeschleust. Diese saugten, erst mal zum Aufladen von Smartphone oder Tablet am PC angesteckt, Daten von dessen Festplatte ab. „Auch das Fernsteuern eines PCs oder die Aktivierung der Kamera sind dadurch möglich“, so Andrijevic.

Alles muss auf den Prüfstand

Das Beispiel zeigt: Firewall und Antivirus-Programm reichen heute längst nicht mehr aus. Es bedarf umfassender Sicherheitslösungen, um auch neuartigen Herausforderungen begegnen zu können. „Die IT-Sicherheit muss mit der Digitalisierung mitwachsen. Alle Geräte, Softwareprogramme und Web-Anwendungen müssen immer wieder auf den IT-Sicherheits-Prüfstand“, rät Andrijevic. Doch was würde nun konkret gegen das manipulierte USB-Kabel helfen? Eine moderne Endpoint-Security-Lösung, sagt Andrijevic. Dieser hat mit dem klassischen Virenscanner nicht mehr viel zu tun, sondern besteht vielmehr aus kombinierten Schutzmechanismen. Dabei wird die Schwarmintelligenz der Cloud genutzt: Die Signatur eines als schädlich eingestuften Programms wird weltweit geteilt. „Eine solche Echtzeitanalytik ermöglicht es, Bedrohungsinformationen allen Nutzern zur Verfügung zu stellen, ohne laufend updaten zu müssen.“ Vor der Ausführung der Datei wird – vereinfacht ausgedrückt – über eine Cloud weltweiter Datenbanken von Virenscannern überprüft, ob der Hashwert des Programms, ein alphanumerischer Wert, als schädlich bekannt ist und nicht installiert werden darf. Ist er das nicht, wird das Programm in die Cloud hochgeladen und in einer Sandbox, einer gesicherten Umgebung, ausgeführt und analysiert. Wurde die Datei dagegen als schädlich eingestuft, wird der Versuch, das für einen Angriff erforderliche Programm auf dem PC zu installieren, als „Anomalie“ gewertet und die Installation unterbunden.

Zu einem sicheren Netzwerk, das den Stand der Technik und den Grad der Vernetzung abbildet, gehören Andrijevic zufolge auch Switches der jüngsten Generation. Der Switch ist ein Verteiler, der die Netzwerksegmente verbindet und Datenpakete an angeschlossene Geräte weiterleitet: Ein herkömmlicher Switch würde es zulassen, dass der mit dem Rechenzentrum des Unternehmens verbundene Mitarbeiter-PC mithilfe des manipulierten Kabels sämtliche Unternehmensdaten unentdeckt herunterlädt. Der moderne Switch hingegen kann die Verbindungsdaten an übergeordnete Systeme übermitteln, die eine solche Datenkommunikation unter Umständen als „Anomalie“ einstufen und dann eine Isolation des Client-Rechners automatisch antriggern und eine Alarmierung veranlassen. Doch selbst die modernste IT-Infrastruktur könne keine 100-prozentige IT-Sicherheit bieten, betont Andrijevic. „Die IT-Sicherheit ist immer so stark wie ihr schwächstes Glied. Das ist meistens der Mensch.“

Angriff per Drohne

Aus Hackersicht noch immer erfolgreich ist die Methode des „verlorenen“ USB-Sticks, die sich die menschliche Neugier zunutze macht. Denn die meisten Menschen, die einen USB-Stick finden, stecken ihn am (Firmen-)PC an und bringen dadurch das Unternehmen in Gefahr. „Eine neue Technologie verleiht dieser altbekannten Angriffsart neue Brisanz: Hacker setzen Drohnen ein, die über die Zugangskontrolle hinweg auf das Firmengelände fliegen und USB-Sticks abwerfen“, sagt Andrijevic. Drohnen eröffneten auch noch weitere Angriffsmöglichkeiten. Kürzlich sei ein Logistikunternehmen angegriffen worden, indem per Drohne ein WLAN-Störsender auf dem Dach der Firma abgestellt worden sei. „Im Lager kommunizierten die Gabelstapler über WLAN und die über 100 Angestellten arbeiteten mit vernetzten Handscannern. Der Störsender legte alles lahm. Die Firma brachte kein einziges Paket mehr hinaus.“

Auf eine andere Sicherheitslücke sei man bei einem Maschinenbauunternehmen gestoßen, berichtet Andrijevic. „Neben der Firma befindet sich eine 24-Stunden-Tankstelle. Ein Tankstellenmitarbeiter hat sein Tablet über ein Netzwerkabel an einer der Videoüberwachungskameras der Firma angeschlossen. Er hatte soweit bekannt keine kriminellen Absichten, sondern wollte einfach nur ins Internet, um sich während der Nachtschicht die Zeit zu vertreiben. Er hätte aber Nacht für Nacht auf alle Unternehmensdaten zugreifen können.“ Auch hier hätte ein moderner Switch mit den entsprechenden Zugangskontrollen zum Unternehmensnetzwerk die Sicherheitslücke zuverlässig geschlossen. „Es zeigt sich immer wieder: Eine moderne Netzwerkinfrastuktur kann für ein Unternehmen überlebenswichtig sein.“

Bewusstsein für IT-Sicherheit ist essenziell für Unternehmen

Über ein umfangreiches Portofolio technischer Schutzlösungen hinaus bietet SWS auch individuelles „Awareness-Training“ an.

Von Stephanie Burger

REGENSBURG. Allen Warnungen und Hinweisen zum Trotz – allzu oft werden unbedacht E-Mail-Anhänge geöffnet, auf Links geklickt und „schlechte“ Passwörter verwendet. Damit kann das Unheil seinen Lauf nehmen. Denn Cyberangriffe erfolgen oft über das schwächste Glied im IT-Sicherheitssystem: den Menschen. „Cybersicherheit steht und fällt mit den Mitarbeitern. Sie bilden sozusagen die letzte Verteidigungslinie. Aus diesem Grund sollten die Sensibilisierung für IT-Sicherheit, regelmäßige Schulungen und auch Know-how-Tests wesentlich zur IT-Strategie jedes Unternehmens gehören“, sagt Markus Leitner, Account Manager bei der SWS Computersysteme AG. Der IT-Dienstleister hat es sich zur Aufgabe gemacht, Bewusstein für IT-Sicherheit in den Unternehmen zu schaffen. Neben einem umfangreichen IT-Sicherheits-Portfolio bietet SWS deshalb auch kundenindividuelles „Awareness-Training“ für Mitarbeiter an.

„An der Schnittstelle zwischen Mensch und IT können zahlreiche sicherheitskritische Situationen entstehen. Deshalb ist es unerlässlich, immer wieder darauf aufmerksam zu machen“, sagt Leitner. So kann beispielsweise der Klick auf einen in einer Phishing-Mail enthaltenen Link ausreichen, um den Anwender-PC mit einer Schadsoftware zu infizieren. Der Link kann aber auch zu einer manipulierten Login-Seite führen, um die Benutzerdaten des Anwenders abzugreifen.

„Auch wenn die IT-Sicherheit technisch auf aktuellem Stand ist, finden Hacker Lücken, die sie gezielt ausnutzen“, sagt Leitner. Beispielsweise werden Websites, die Schadsoftware beherbergen, nach einigen Stunden wieder stillgelegt und unter anderer Adresse eröffnet. „Da greift der technische Schutz nicht.“ Genauso, wie der technische Schutz stets aktuell gehalten werden müsse, gelte es auch, die Mitarbeiter auf den neuesten Kenntnisstand zu bringen. Ein aktuelles Thema in vielen Unternehmen sei beispielsweise auch das Mobile Device Management, also der sichere und transparente Umgang mit Smartphones und Tablets im Unternehmen.

Ziel des „Awareness-Trainings“ sei aber vor allem, bei den Mitarbeitern Akzeptanz und ein positives Image für die IT-Sicherheitsmaßnahmen zu erzeugen. „Denn wenn womöglich der moderne Virenscanner den PC langsamer macht, dann stößt das sehr schnell auf Unmut. Als Dienstleister suchen wir immer den Mittelweg zwischen Benutzerfreundlichkeit und Sicherheit“, sagt Leitner.

Zur „Awareness“ gehöre es auch, dass Mitarbeiter ermutigt werden, Fehler einzugestehen. „Niemand ist davor sicher. Für Angreifer ist es oft einfacher, über den Menschen zu gehen, als zu versuchen, die technischen Schutzmaßnahmen zu überwinden.“ Social-Engineering-Attacken, bei denen versucht wird, sich das Vertrauen von Mitarbeitern zu erschleichen und menschliche Schwächen wie Gier, Angst oder Autoritätshörigkeit auszunutzen, werden Leitner zufolge immer raffinierter. Der häufigste Angriffsvektor ist dabei nach wie vor die E-Mail. Um die Empfänger mit einer E-Mail zu einer Aktion zu bewegen, werden – anders als in den breit gestreuten und relativ leicht zu entlarvenden Spam-Mails – die „Köder“ aufwendig gestaltet und auf eine bestimmte Zielgruppe zugeschnitten.

„Gerade das Social Engineering zeigt sehr deutlich, dass Mitarbeiter ein kritischer Faktor der IT-Sicherheit sind. Hier hilft nur ein Mittel: Awareness schaffen, auf allen Ebenen eines Unternehmens“, betont Leitner.

Das kleine blaue Schloss, das Account Manager Markus Leitner in der Hand hält, steht bei SWS für „IT-Sicherheit“. Foto: Attila Henning

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