Advertorial

SWS COMPUTERSYSTEME

Mit ihren IT-Experten sorgen sie für mehr Sicherheit in der digitalen Welt: Lothar Fesl, Vorstand und Christian Schreiner, Vorstandsvorsitzender der SWS Computersysteme AG. Foto: Andre Dünnbier

So wappnen sich Firmen gegen Cyberattacken

Daten sind Kronjuwelen im digitalen Zeitalter. Um sie zu schützen, müssen Unternehmen vorbereitet sein und in Sicherheitsmechanismen investieren.

Von Julia Kellner

REGENSBURG/HAUZENBERG. Automatisierung, Online-Angebote, Zugriff aus aller Welt: Unternehmen digitalisieren ihre Prozesse und Services, um auf dem Markt bestehen zu können. Sie sind mit ihren Kunden, Geschäftspartnern und Mitarbeitern virtuell verbunden. Seit der Coronakrise entwickelt sich die Digitalisierung im Turbotempo. Der Datenberg wächst, jede Sekunde – damit steigen auch die potenziellen Angriffsszenarien für Cyberkriminelle.

Datenschutz ist Chefsache

Dennoch bleibt oft die IT-Sicherheit auf der Strecke. „Unternehmen müssen ihre Kronjuwelen – also ihr wertvolles Know-how, ihre Firmen- und Personendaten – vor unerwünschten Angriffen schützen“, sagt Hans-Martin Kuhn, IT-Securityexperte bei SWS Computersysteme. Schließlich seien die Folgen des Datenklaus oft nicht kalkulierbar: Umsatzeinbußen, Imageschäden, Vertrauensverlust und massive Beeinträchtigungen von Geschäftsprozessen.

Dass Cyberangriffe unbedingt abgewehrt werden müssen, zeigen auch die empfindlichen Strafen, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) verhängt. Laut Kuhn müssen Unternehmen, die einen IT-Sicherheitsvorfall mit personenbezogenen Daten haben und ihrer Meldepflicht nicht innerhalb von 72 Stunden nachkommen, mit Bußgeldern von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes rechnen. „Die Geschäftsführer sind in der Pflicht, sie haften mit ihrem Privatvermögen.“ IT-Abteilungen müssten deshalb regelmäßig ihre Istsituation genau analysieren und mögliche Schwachstellen in der IT-Landschaft aufdecken.

Eine komplexe Aufgabe, bei der SWS mit ihrem Security-Operation-Center unterstütze. Schließlich seien die Angriffsflächen für Cyberkriminelle vielfältig. „Sie versuchen es beispielsweise mit Phishingattacken: Dabei fallen Mitarbeiter oft auf Mails mit Schadsoftware herein.“ Wenn ein Computer oder Netzwerk dabei mit Ransomware infiziert wurde, blockiere es den Systemzugang oder verschlüsselt Daten. Von hier an unterscheide sich der Angriff nicht mehr von jedem anderen Erpressungsfall: Für die Freigabe wird Lösegeld gefordert.

Sogenannte Denial-of-Service-Angriffe könnten sogar die gesamte Firma lahmlegen. „Sie richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen.“ Selbst kleine Firmen seien vor gefährlichen Angriffen nicht gefeit. „Cybercrime kann jeden treffen“, sagt der IT-Sicherheitsexperte. Denn kriminelle Banden nutzten oft Massenmailings und würden jedes Ziel angreifen. Mittlerweile gebe es im Darknet sogar professionelle Tools, mit denen Hacker für kleines Geld Zugriffsdaten abgreifen.

Für ihre Kunden aus den unterschiedlichsten Branchen decke SWS Computersysteme genau diese und viele weitere Schwachstellen auf – mittels Security Audits und Penetrationtests. Weil die IT-Umgebung immer komplexer wird, seien Sicherheitslücken auf nahezu allen Geräten verteilt. Auch das Arbeiten im Homeoffice und die Datenspeicherung in der Cloud schaffe neue Angriffsmöglichkeiten. Das Bundesamt für Informationssicherheit fordere deshalb Sicherheitsmechanismen auf dem aktuellsten Stand der Technik. „Der Schutz vor Cyberattacken ist ein ständiger Balanceakt zwischen Sicherheit, Benutzerfreundlichkeit und Funktionsfähigkeit“, erklärt Hans-Martin Kuhn.

IT-Sicherheit ist kein Projekt, sondern ein Prozess

Um die IT-Sicherheit seiner Kunden nachhaltig zu gewährleisten, überprüfe SWS regelmäßig alle Systeme. Sie setze auf einen ganzheitlichen Ansatz, einen vielfältigen Werkzeugkasten, der Sicherheitslücken schließt. Dazu gehöre etwa eine Multi-Faktor-Authentifizierung: Für Mitarbeiter ist der Zugriff nur über eine mehrfache Registrierung möglich. Mittels verschiedener Mechanismen können Kuhn zufolge Anomalien erkannt werden. Beispielsweise dann, wenn sich jemand zunächst in Regensburg ins Firmennetz einloggt und schon eine halbe Stunde später in Berlin. „Der Zugriff wird dann blockiert.“

Zunehmend arbeite man mit sogenannten Zero-Trust-Lösungen. „Im Prinzip geht es darum, dass keinem Akteur vertraut wird: Jeder Zugriff wird individuell authentifiziert“, sagt Kuhn. Zwar gebe es keinen hundertprozentigen Schutz vor Cyberattacken, doch umso höher die Hürden, desto geringer sei die Bedrohung. „Haben es Hacker schwer, ziehen sie zum nächsten weiter.“ Genauso wichtig, oder sogar noch wichtiger, wie die technische Komponente ist laut Kuhn der Faktor Mensch. Nötig sei ein gesteigertes Bewusstsein. Er nennt es die „menschliche Firewall“. Für den richtigen Umgang mit digitalen Bedrohungen bietet SWS deshalb Schulungen und simulierte Phishingangriffe. Sie sollen Mitarbeiter für digitale Gefahren sensibilisieren.

In Echtzeit: Auftragshacker zeigt IT-Schwachstellen auf

Um Firmen fit für die digitale Welt zu machen, lädt SWS am 7. Juli zur Messe „BrainShare“ in Hauzenberg. Im Fokus: IT-Sicherheit.

Von Julia Kellner

HAUZENBERG. Ein paar Klicks, wenige Minuten, Daten weg. Philipp Kalweit findet Fehler im System. Als Deutschlands jüngster Auftragshacker spürt er IT-Schwachstellen für Unternehmen auf. Seine Mission: mehr Sicherheit für die digitale Welt. Wie einfach es ist, wertvolle Daten abzugreifen, zeigt Kalweit sogar im Livemodus: Am 7. Juli ist er als Redner zu Gast bei der IT-Messe „BrainShare“ von SWS Computersysteme. Schon seit 20 Jahren lädt das Unternehmen jährlich zu diesem Event – diesmal nach Hauzenberg im Landkreis Passau. Dort wurde kürzlich das neue Firmengebäude eröffnet mit Platz für 150 Arbeitsplätze, Seminare und öffentliche Kulturveranstaltungen. Rund 450 Teilnehmer durfte SWS bei den vergangenen Veranstaltungen begrüßen.

Dass nach zweijähriger Corona-Pause viele Themen rund um IT-Sicherheit im Fokus stehen, ist kein Zufall. „Cyberangriffe sind seit der Pandemie angestiegen, Hacker nutzen gängige Schwachstellen aus, beispielsweise bei der vermehrten Datenspeicherung in der Cloud oder aus der Umstellung auf Remotearbeit“, sagt Hans-Martin Kuhn, IT-Securityexperte bei SWS Computersysteme. Besonders der Trend zum Homeoffice zeige das Dilemma, in dem die Informationssicherheit stecke: Dank neuer Technologien und flexibler Arbeitsmodelle können vertrauliche Daten leichter den geschützten Bereich verlassen. „Für Firmen ist es eine Gratwanderung – sie müssen Richtlinien definieren, die innerhalb der privaten IT-Infrastruktur der Mitarbeiter gelten.“ Um die Sicherheitslücken möglichst zu minimieren, dürfe beispielsweise nur über Hardware, die der Arbeitgeber zur Verfügung stellt, und eine sichere VPN-Verbindung auf Firmendaten zugegriffen werden. Die Veranstaltung sei auch deshalb so bedeutend, weil insbesondere der Mensch selbst die größte Schwachstelle in der IT-Sicherheit ist. „Mit BrainShare sensibilisieren wir unsere Gäste für die Bedrohungen in der digitalen Welt“, sagt Jennifer Fesl von SWS, die als Marketingmitarbeiterin den Messetag organisiert. In Fachvorträgen zeigen die Experten der SWS Computersysteme AG reale Gefahren und gleichzeitig Lösungen, um IT-Sicherheitslücken zu schließen. Auch im Messebereich versammeln sich Kooperationspartner, die allesamt Spezialisten in Sachen Cybersicherheit sind.

Abseits der IT-Welt spricht im Abendprogramm Urs Meier zum Thema „Zwischen den Fronten – Entscheidungen unter Druck treffen“. Als Weltschiedsrichter, Unternehmer und Fußballexperte ist er es gewohnt, in Sekundenschnelle zu reagieren. Eine Fähigkeit, die für Unternehmen aller Branchen und ihre Mitarbeiter in Zeiten der Digitalisierung ebenso bedeutsam ist.

Ob SWS-Kunde, interessierte Unternehmerinnen und Unternehmer oder IT-Verantwortliche: Wer zur Hausmesse nach Hauzenberg kommen möchte, meldet sich auf www.sws.de/brainshare an. „Gerne auch kurzfristig – etwa eine Woche vor Messebeginn sollte die Anmeldung eingegangen sein“, sagt Fesl. Der Messetag ist völlig kostenlos. Teilnehmer dürfen sich ab 10.30 Uhr bis in die späten Abendstunden auf ein buntes Programm freuen – Moderation, Musik, Essen und Trinken inklusive. Jeder, der den Weg zum Arbeiten unterwegs oder einfach nur zum Relaxen nutzen möchte, steigt in einen der Shuttlebusse. „Sie fahren von Nürnberg und Regensburg aus in unser Headquarter nach Hauzenberg und wieder zurück.“ Fahrtickets dafür gibt es kostenfrei, gebucht werden sie zusammen mit der Online-Anmeldung.

Bei der Hausmesse „BrainShare“ am 7. Juli zeigt SWS, wie sich Unternehmer vor Hackerangriffen schützen können. Foto: SWS Computersysteme AG

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