WZ-Serie

DIGITALISIERUNG – ABER SICHER!

Die Digitalisierung bestimmt zunehmend auch die Fertigung – IT-Sicherheit wird damit umso wichtiger. Fotos: SWS

Cyber-Abwehr nach Maß

SWS realisiert kundenindividuelle IT-Security-Lösungen für jede Branche.

Von Stephanie Burger

REGENSBURG. Erpressersoftware, Industriespionage oder Social Engineering – die Sicherheitsrisiken für Unternehmen werden immer zahlreicher. Die Gefährdungslage sei nach wie vor „auf hohem Niveau angespannt“, stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Anfang November vorgestellten Lagebericht fest. Vor allem die zunehmende Verlagerung von Diensten ins Internet öffnet Cyberkriminellen immer mehr Einfallstore. „So vielfältig die Möglichkeiten der Digitalisierung auch sind, so groß sind auch die damit einhergehenden Gefahren“, sagt Martin Kopp, Security Operations Center (SOC) Manager bei SWS, einem Systemhaus, das sich auf die IT-Strukturen des Mittelstandes spezialisiert hat. Bedroht sind nicht nur Konzerne oder große Industriebetriebe, sondern auch kleine und mittlere Unternehmen. „Von Cyberkriminellen gestohlene Konstruktionspläne sind keine Seltenheit“, sagt Kopp. Doch die Digitalisierung müsse nicht auf Kosten der IT-Sicherheit gehen. Diese sei vielmehr die notwendige Voraussetzung für die digitale Transformation, betont Kopp.

Gefahr durch Ransomware

Laut dem IT-Security-Experten verursachen aktuell vor allem drei Gefahrentrends Probleme. Zum einen Ransomware, eine Erpressungs- oder Verschlüsselungssoftware, die Computer sperrt oder darauf befindliche Daten verschlüsselt und für die Entschlüsselung Lösegeld fordert – oder oft auch „nur“ Schaden anrichtet. Die letzte digitale Rechner-Geiselnahme liegt nur wenige Monate zurück: „NotPetya“ griff die Containerterminals einer dänischen Reederei an. Ein deutlicher Rückgang des Handelsvolumens und einige hundert Millionen Dollar Schaden waren die Folgen. „Allein der Schaden durch den Produktionsausfall kann existenzbedrohend sein – auch ohne Erpressungsversuch“, sagt Kopp.

Ein weiterer Gefahrentrend sind sogenannte DDoS-Angriffe. DDoS steht für Distributed Denial of Service. Dabei überflutet eine Vielzahl von Angreifern in einer konzertierten Aktion den Server mit Anfragen, bis er überlastet ist und den Dienst versagt. Ausgeführt werden solche Attacken oft von einem Botnetz, einem Zusammenschluss von mit Schadprogrammen versehenen Computern „unschuldiger“ Benutzer. Aber auch vernetzte elektronische Geräte wie Lampen, Fernseher oder Telefone können dafür missbraucht werden. Eine dritte große Gefahr ist die Industriespionage, die oft mit „Social Engineering“ in Verbindung steht. „Dabei werden menschliche Schwächen skrupellos ausgenutzt. Ein Anrufer gibt sich zum Beispiel als Kollege einer anderen Filiale aus und bittet um Zusendung eines Passwortes. Ein plumper Täuschungsversuch, der dennoch oft zum Erfolg führt, weil das Bewusstsein für IT-Sicherheit immer noch zu wenig ausgeprägt ist“, so Kopp.

Dieses zu wecken, hat sich SWS auf die Fahnen geschrieben. Die Sensibilisierung ist ein wesentlicher Bestandteil des ganzheitlichen Verständnisses von IT-Sicherheit, für das SWS steht. Als IT-Security-Partner unterstützt SWS Kunden dabei, Security als fortlaufenden Prozess im Unternehmen zu verankern. Der Fokus des Regensburger Unternehmens liegt dabei auf dem Mittelstand: Zu den Kunden zählen unter anderem Maschinenbauer, Kliniken, Versicherungen, Behörden und auch die Betreiber kritischer Infrastrukturen (KRITIS) wie zum Beispiel Energieversorger. „Wichtig ist es uns, maßgeschneiderte und bedarfsorientierte Lösungen umzusetzen“, betont SWS-Key-Account-Manager Markus Leitner. In einem ausführlichen Beratungsgespräch werden deshalb zunächst der Ist-Zustand und mögliche Sicherheitsschwachstellen erhoben und in einem weiteren Schritt Handlungsempfehlungen und Maßnahmen abgeleitet – zunächst auf organisatorischer Ebene, das heißt in Form von Anweisungen oder Richtlinien. Darauf abgestimmt wird eine Reihe technischer Schutzmaßnahmen definiert. SWS bietet ein umfassendes Portfolio bewährter Sicherheitsprodukte. „Der Mount Everest der IT-Sicherheit ist sicherlich ein Informationssicherheitsmanagementsystem, das aber für einen Betrieb mit 20 Mitarbeitern kaum wirtschaftlich abgebildet werden kann. Hier kommt unsere Kernkompetenz ins Spiel, nämlich ein IT-Sicherheitskonzept so zu skalieren, dass es exakt den Anforderungen des Kunden entspricht“, erklärt Leitner.

Betreibermodell oder Cloud

SWS bietet dabei viele IT-Dienste entweder als Managed Service, das heißt als Betreibermodell, bei dem der Kunde zwar die installierten Geräte erwirbt, aber der Dienstleister die Verantwortung für die Bereitstellung der definierten Dienste übernimmt, oder als Cloud Service an. Wählt der Kunde diese Option, laufen die Dienste, die er nutzt, auf den zugangsgeschützten Servern im Rechenzentrum der SWS. Der Kunde muss nichts mehr kaufen, er bezahlt vielmehr für die Nutzung von Diensten. Für welche Lösung man sich auch entscheidet – Tatsache ist, dass die IT-Sicherheits-Anforderungen in Zeiten der Digitalisierung weiter steigen. „Das Internet der Dinge und die Vernetzung der Produktion bringen neue Gefahren. Immer mehr Geräte sind internetfähig und müssen gesichert werden. Heute ist beispielsweise der Netzwerkdrucker eine noch immer unterschätzte Sicherheitslücke, in zwei Jahren wird vielleicht der Kühlschrank zum Risiko“, warnt Kopp.

Das „S“ symbolisiert den ganzheitlichen IT-Security-Ansatz von SWS.

INTERVIEW

Gespräch mit Christian Schreiner, Vorstandsvorsitzender der SWS Computersysteme AG

Auch der Mittelstand ist nicht vor Spionage sicher

Herr Schreiner, wächst mit der Digitalisierung die Bedeutung der IT-Sicherheit?

Christian Schreiner: Ja, das kann man definitiv sagen. Fast täglich werden Firmennetzwerke aus dem Dunkel des Cyberspace angegriffen. Die Bedrohungslage hält an. IT-Sicherheit ist kein nachträglicher Aspekt, der im Zuge der Digitalisierung auch noch berücksichtigt werden muss, sondern die Voraussetzung für Digitalisierung. Beides muss Hand in Hand gehen.

> ***„Die Sensibilisierung der Belegschaft für IT-Sicherheit ist ganz zentral. Denn die Bedrohungen kommen eben nicht nur von außen, sondern sehr oft auch von innen.“***
>
> Christian Schreiner

Die digitale Transformation im Unternehmen voranzutreiben und gleichzeitig die IT-Sicherheit nicht zu vernachlässigen, stellt für viele Unternehmen eine erhebliche Herausforderung dar. Wie geht man beide Themen konzertiert an?

Wir empfehlen ein modulares Vorgehen, das exakt an die Bedürfnisse eines Unternehmens angepasst ist. Zunächst sollten die offensichtlichsten Sicherheitslücken geschlossen werden. Wir überprüfen natürlich auch, ob Basismaßnahmen wie Firewall und Backup vorhanden sind. Danach sollte jeder neue digitale Prozess, der Einzug hält, immer auch unter dem Aspekt der Security analysiert werden, um ihn von vornherein sicher zu machen. Alle Maßnahmen müssen außerdem einem kontinuierlichen Verbesserungsprozess unterliegen. Es geht dabei auch immer um die perfekte Balance zwischen IT-Sicherheit und reibungslos ablaufenden Geschäftsprozessen. Dieses Gleichgewicht für unsere Kunden herzustellen, gehört zu unserer Kernkompetenz.

Die IT-Sicherheitsanforderungen werden immer höher. Kann man diesen ohne Outsourcing und externe Dienstleister überhaupt noch gerecht werden?

Das wird in der Tat immer schwieriger. Aber es gibt gut skalierbare Lösungen, je nach individuellen Voraussetzungen und Bedürfnissen. Ein Sicherheitskonzept kann nicht einfach übergestülpt werden, es muss Schritt für Schritt entstehen. Unser Ansatz beginnt deshalb mit einer Analyse. Hier sehen wir uns mit dem Kunden alle Prozesse an und stellen die neuralgischen Punkte fest. Erst danach geht es um die Lösungen, und zwar um technische und organisatorische. Die besten IT-Security-Produkte nützen nicht viel, wenn sie nicht in ein organisatorisches Konzept eingebunden sind.

Ihr Anliegen ist es auch, das Bewusstsein für IT-Sicherheit zu schärfen. Warum ist Ihnen das so wichtig?

Es ist ein Thema, das beim Einzelnen beginnt. Wenn jemand als Privatperson kein IT-Sicherheitsbewusstsein hat, dann legt er auch als Arbeitnehmer kaum ein solches an den Tag. Die Sensibilisierung der Belegschaft für dieses Thema ist deshalb ganz zentral. Denn die Bedrohungen kommen eben nicht nur von außen, sondern sehr oft auch von innen. Ein plakatives Beispiel: Im Rahmen einer Studie haben 2016 zwei US-amerikanische Universitäten und Google USB-Sticks als Köder vor verschiedenen Firmenzentralen ausgelegt. Rund die Hälfte der Finder nahm den Stick mit, schloss ihn in seiner Firma an einen Computer an und öffnete Dateien. So leicht kann Malware ins Unternehmen gelangen.

Was sind die größten Hemmnisse bei der IT-Sicherheit?

Zum einen das fehlende Wissen, was mit der Komplexität der Thematik zu tun hat. Zum anderen aber auch die mangelnde Bereitschaft, Geld prophylaktisch zu investieren. Oft ist Investitionsbereitschaft erst dann vorhanden, wenn ein Schadensfall eingetreten ist.

Wie groß ist die Gefahr, als mittelständisches Unternehmen Opfer von Industriespionage zu werden?

Gerade unser innovativer Mittelstand ist gefährdet. Es ist keine Seltenheit, dass ein Unternehmen bei der Patentanmeldung feststellen muss, dass ein chinesischer Konzern mit demselben Patent einen Tag früher dran war. Aber auch verlorene Ausschreibungen aufgrund ausgespähter Preisgestaltung sorgen immer wieder für geschäftliche Rückschläge.

Interview: Stephanie Burger
Foto: SWS

KONTAKT

SWS Computersysteme AG
Brünstraße 2 | 94051 Hauzenberg
Telefon: +49 (0) 8586 / 9604-0
info@sws.de | www.sws.de

Standort Regensburg:
Im Gewerbepark D 75
93059 Regensburg
Telefon: +49 (0) 941 / 20605-0