WZ-Serie

# DIGITALISIERUNG – ABER SICHER!

SWS COMPUTERSYSTEME
Member of ACP Group

INTERVIEW

Gespräch mit Christian Schreiner, Vorstandsvorsitzender der SWS Computersysteme AG

## IT-Security ist Chefsache

*Herr Schreiner, Sie sagen, IT-Security ist Chefsache. Warum?*

Christian Schreiner: Weil es extrem wichtig ist, Mitarbeiter zu sensibilisieren und zu informieren. Zum Beispiel darüber, dass ein gefundener USB-Stick nicht ohne Überprüfung verwendet werden darf oder das private Notebook im Firmennetz nichts zu suchen hat. Das kleine Security-Einmaleins muss den Mitarbeitern vermittelt werden. Es bringt schließlich nichts, wenn die IT-Abteilung das Unternehmen wie Fort Knox absichert, die Mitarbeiter aber dann die Fenster offen lassen. Ein Sicherheitsbeauftragter kann zum Beispiel alle notwendigen Maßnahmen anstoßen und kontrollieren. All dies kann allerdings nur die Unternehmensführung veranlassen und die muss dann mit gutem Beispiel vorangehen und dranbleiben. IT-Security ist kein einmaliges Projekt, sondern ein fortlaufender Prozess.

*Vor den rechtlichen Aspekten kann sich ein Firmenchef wohl nicht verstecken?*

So ist es. Vorgaben des Gesetzgebers und nicht zuletzt der Datenschutz verlangen von Unternehmen, ihre Sicherheitskonzepte kontinuierlich an die aktuellen Gegebenheiten anzupassen. Hier gilt es, die Sicherheitsstandards im Unternehmen immer wieder zu überprüfen. Denn die Hackerszene schläft nicht. Fast täglich entstehen neue Bedrohungen, neue Angriffsvarianten und das bedarf einer kontinuierlichen Anpassung der Sicherheitsstrategie. Das erfordert Einsatz und Mitwirken aller Mitarbeiter und als Voraussetzung das Verständnis und die Unterstützung der Geschäftsführung.

*Was sind die derzeit gängigsten Arten von Hackerangriffen?*

Das ist nach wie vor die „Geiselnahme von Daten", das heißt deren Verschlüsselung und die Forderung eines „Lösegelds" für die Entschlüsselung. Die entsprechenden Geschichten, die durch die Presse geistern, sind keine Panikmache und betreffen auch nicht nur Großkonzerne. Wir erleben regelmäßig, dass auch kleine Unternehmen sowie Mittelständler und sogar Privatpersonen dieser Masche zum Opfer fallen. Dahinter stecken meist kriminelle, organisierte Hackerringe.

*Wie kommen Hacker an sensible Daten?*

Meist durch schlechte Systempflege! Wenn nicht regelmäßig Updates installiert und die Sicherheit der Systeme überprüft werden, entstehen Lücken, die Hacker buchstäblich zum Angriff einladen. In vielen Fällen warten sie sogar darauf. Angriffe werden zunehmend individualisierter und gehen nicht mehr nur von Hobbyhackern aus, sondern auch von ausländischen Geheimdiensten. Für Cyberkriminelle führt der kürzeste Weg zu Unternehmensdaten über Anwendungen – und der Schlüssel zu diesen Anwendungen sind gestohlene Nutzer-IDs. Veraltete oder falsche Sicherheitsmaßnahmen mit herkömmlichen Netzwerkfirewalls sind längst nicht mehr in der Lage, Angriffe dieser Art zu stoppen.

*Was setzen Sie als Securityspezialist dieser Gefahr entgegen?*

Neue bedrohungsorientierte und dynamische Securitykonzepte beinhalten ein Zusammenspiel mehrerer Sicherheitskomponenten, die Informationen in Korrelation setzen. Wir nutzen beispielsweise moderne, globale Gefahren- und Bedrohungsdatenbanken online. Wird zum Beispiel in China ein Gerät mit einem bestimmten Schadcode angegriffen, ist dieser nach Analyse eine Minute später schon in der Gefahrendatenbank gespeichert.

**Christian Schreiner**
Vorstandsvorsitzender
der SWS Computersysteme AG

Unsere Systeme nutzen diese Informationen online und können einen entsprechenden Angriff folglich sofort abwehren. Dabei helfen moderne Next Generation Firewalls, die Daten und Benutzeridentitäten besonders effektiv schützen. Moderne IT-Security ist also wie ein Puzzle. Eine Anwendung greift in die andere und ist nur im Gesamtbild stark.

*Welche Vorsichtsmaßnahmen können Unternehmen selbst installieren?*

Zunächst ist es wichtig, zu überlegen, wer wann Zugriff auf welche sensiblen Daten braucht. Hier müssen sinnvolle und strikte Regeln eingeführt werden, um unnötige Sicherheitsrisiken einzudämmen. Zudem müssen Mitarbeiter hinsichtlich aller Gefahren ihres digitalen Handelns sensibilisiert und geschult werden. Für den Krisenfall müssen Notfallszenarien erarbeitet werden, die eine schnelle Reaktion ermöglichen. Denn Fakt ist, wirklich jede Organisation ist schon einmal Opfer einer versuchten Cyberattacke geworden oder steht im Fadenkreuz von Hackern. Das ist eine ganz reale Gefahr. Die Frage ist grundsätzlich nicht, ob, sondern wann es passiert ist und welcher Schaden angerichtet wurde.

*Interview: Julia Rummel*
*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


**Wer mit digitalen Geschäftsmodellen Erfolg haben möchte, muss die Sicherheitsrisiken kennen und entsprechende Securitylösungen finden.** Illustration: Robert Kneschke - stock.adobe.com

# Digitale Geschäftsmodelle – digitale Bedrohungen

Die SWS AG stellt sich mit individuellen Securitylösungen Hackern entgegen.

Von Julia Rummel

**REGENSBURG.** Früher war alles besser. Zumindest aus IT-Security-Sicht stimmt das. Die komplette IT-Landschaft war im firmeneigenen Rechenzentrum angesiedelt, Maschinen waren kaum miteinander vernetzt, Produktions- und Verwaltungssysteme getrennt und Daten verließen nur selten ihre Silos, geschweige denn die Grenzen des eigenen Firmengeländes. Diese Daten wurden von den Usern über lokale Netzwerke direkt ausgetauscht. Sicherheit bedeutete, die Netzwerke und Server mit starken Firewalls vor Gefahren von außen zu schützen. Das war in erster Linie Aufgabe der IT-Abteilung und stellte kein großes Problem dar, denn sie hatte alles im Blick sowie die totale Kontrolle über die eingesetzte Hard- und Software.

### Hackerattacken sind unvermeidlich

Das alles ist nun Schnee von gestern: Unternehmensnetzwerke haben heute enorm viele Schnittstellen, also Ein- und Ausgänge, Maschinen und Produktionsanlagen sind mit IT-Anwendungen verbunden und werden oftmals sogar über das Internet gesteuert und gewartet. Externe Dienstleister und Partner haben zum Teil Zugriff auf Geschäfts- und Kundendaten. Gearbeitet wird heute nicht mehr nur in der Firma, sondern überall – im Homeoffice oder unterwegs per Smartphone und Tablet. Herkömmliche Anwendungen sind durch webbasierte, mobile oder durch Software-as-a-Service-Anwendungen wie Office 365 ersetzt worden. Vertrauliche Daten werden so nicht mehr ausschließlich aus speziell gesicherten Firmennetzen abgerufen, sondern häufig auch über ungesicherte Netzwerkverbindungen wie öffentliche WLAN-Hotspots an Flughäfen oder in Zügen. Zudem mischen viele Mitarbeiter private und Firmendaten auf diversen Endgeräten und nutzen schwache, veraltete oder identische Passwörter für verschiedene Systeme. Zudem werden oft vertrauliche Unternehmensinformationen mit nicht genehmigten Anwendungen wie Dropbox oder Skype an Kollegen und Kunden versendet.

In einer vernetzten Welt sind die ehemals geschlossenen Systeme der Unternehmen neuen beziehungsweise veränderten Bedrohungen ausgesetzt. Klar ist: Den Wachstumsmöglichkeiten durch digitale Geschäftsmodelle und neue Arbeitswelten stehen auch neue, mächtige Risiken gegenüber. Hackerattacken auf Unternehmen sind heute unvermeidbar. Allein die Qualität des jeweiligen individuellen IT-Sicherheitskonzepts entscheidet, ob ein Angriff erfolgreich beziehungsweise wie groß der Schaden sein wird.

Damit der Schaden möglichst gering ausfällt beziehungsweise von vornherein ausbleibt, setzen sich die IT-Security-Experten der SWS Computersysteme AG täglich an die Entwicklung entsprechend hochwertiger und immer auch individuell angepasster Sicherheitskonzepte. Dabei stellen sie sich auf jedes Unternehmen genau ein und gehen bei der Auslotung aller Sicherheitsrisiken und Anforderungen präzise vor. Schließlich gilt es, das jeweilige Unternehmen aus der Sicht eines potenziellen Angreifers aus dem Cyberspace zu analysieren, um das passende Schutzkonzept zu etablieren. Und das wird immer schwieriger. Denn im Vergleich zu früher haben sich aufgrund der hohen Komplexität nicht nur die Angriffsflächen und damit auch die Risiken erhöht, sondern vor allem auch die Ziele. Diese sind heute nicht mehr nur Netzwerke selbst, sondern nicht zuletzt Unternehmensdaten. Denn diese gehören derzeit zum wertvollsten Gut einer Firma. Nicht umsonst nennt die IT-Branche Daten das Gold des digitalen Zeitalters. Sie sind der Treiber für neues Wachstum. Ihre Sammlung und Auswertung über Abteilungs- und Unternehmensgrenzen hinweg sind Grundlage für die Neuausrichtung sowie die Optimierung von Produktionsprozessen und ermöglichen die Entwicklung neuer Geschäftsmodelle.

### Sicherung des digitalen Goldes

Eine Basisabsicherung mit Virenscanner, Firewall und Passwortschutz ist nicht mehr ausreichend. Moderne Sicherheitssysteme nutzen spezielle Analyseverfahren für die Erkennung und Abwehr von Angriffen, die Verschlüsselung sensibler Daten und die Identifikation der Nutzer. Wer sich hierzu keine ausgefeilte, professionelle und individuell angepasste Securitylösung vom Experten besorgt, spart am falschen Ende und setzt gegebenenfalls die Zukunft seines Unternehmens aufs Spiel. Erfolgreiche Cyberattacken führen zum Teil zu signifikanten wirtschaftlichen Einbußen und Vertrauensverlust bei Kunden sowie Partnern und beschädigen die Unternehmensreputation am Markt nachhaltig. Wer mit digitalen Geschäftsmodellen Erfolg haben möchte, muss seine Sicherheitsrisiken kennen und berücksichtigen, das heißt, Wachstumsstrategien gehen Hand in Hand mit Sicherheitsstrategien. Die Verantwortung hierfür liegt deshalb nicht allein bei der IT-Abteilung, sondern betrifft auch die Unternehmensführung.

**Moderne Sicherheitssysteme dienen der Verschlüsselung sensibler Daten und der Identifikation der Nutzer.** Foto: sonjanovak - stock.adobe.com