SWS
COMPUTERSYSTEME
Member of ACP Group

Digitale Zukunft – Digitale Bedrohungen

IT-Security ist Chefsache

DIGITALE GESCHÄFTSMODELLE – DIGITALE BEDROHUNGEN
Machen Sie Ihre IT-Security zur Chefsache

FRÜHER WAR ALLES BESSER

Zumindest aus IT-Security-Sicht: 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.

Daten wurden über lokale Netzwerke ausgetauscht, von Benutzern, die direkt mit dem Netzwerk verbunden waren. 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 Hardware und Software.

HEUTE SIEHT UNSERE WELT VOLLKOMMEN ANDERS AUS

Im IoT-Zeitalter versprechen innovative Geschäftsmodelle und Arbeitsmethoden neues Wachstum. Unternehmensnetzwerke sind nun offen, Maschinen mit IT-Anwendungen verbunden und Produktionsanlagen werden 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 Home-Office oder unterwegs per Smartphone. Herkömmliche Anwendungen sind webbasiert und mobil oder durch Software-as-a-Service-Anwendungen wie Office 365 oder Salesforce ersetzt. 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 Daten und Firmendaten auf diversen Geräten und nutzen schwache, veraltete oder identische Passwörter für verschiedene Systeme. Oft werden vertrauliche Unternehmensinformationen mit im Zweifelsfall nicht genehmigten Anwendungen wie Dropbox oder Skype an Mitarbeiter und Kollegen versendet.

NEUE GESCHÄFTSMODELLE BEDEUTEN NEUE GEFAHREN

In einer vernetzten Welt sind die ehemals geschlossenen Systeme der Unternehmen neuen bzw. veränderten Bedrohungen ausgesetzt. Klar ist oder sollte sein: Den Wachstumsmöglichkeiten durch digitale Geschäftsmodelle und neue Arbeitswelten stehen neue Risiken gegenüber.

Hackerattacken auf Unternehmen waren und sind unvermeidbar, die Qualität des IT-Sicherheitskonzepts eines Unternehmens entscheidet damals wie heute, ob ein Angriff erfolgreich bzw. wie groß der Schaden ist. Im Vergleich zu früher haben sich allerdings aufgrund der hohen Komplexität nicht nur die Angriffsflächen und damit auch die Risiken vergrößert, sondern auch die Ziele. Attacken zielen heute nicht mehr nur auf die Netzwerke selbst ab, sondern haben nicht zuletzt die Daten im Visier. Denn Daten gehören zum wertvollsten Gut in Unternehmen, sie sind der Treiber für neues Wachstum. Ihre Sammlung und Auswertung über Abteilungs- und Unternehmensgrenzen hinweg sind Grundlage für die Neuausrichtung und Optimierung von Produktionsprozessen und ermöglichen die Entwicklung neuer Geschäftsmodelle.

Für Cyber-Kriminelle 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 nicht in der Lage, Angriffe dieser Art zu stoppen. Neue bedrohungsorientierte und dynamische Security-Konzepte beinhalten Next Generation Firewalls und schützen so auch vor Angriffen auf Daten und Benutzeridentitäten, die auf dem Applikations-Level stattfinden.

T-SECURITY IST CHEFSACHE

Fakt ist, jede Organisation ist schon einmal Opfer einer versuchten Cyberattacke geworden oder steht im Fadenkreuz von Hackern. Unternehmen, die solche sehr realen Gefahren ignorieren oder bei IT-Sicherheit sparen, setzen ihre Zukunft aufs Spiel.

Erfolgreiche Cyberattacken führen zu zum Teil signifikanten wirtschaftlichen Einbußen, Vertrauensverlust bei Kunden und Partnern und beschädigen die Unternehmensreputation im Markt nachhaltig.

Wer mit digitalen Geschäftsmodellen Erfolg haben möchte, muss seine Sicherheitsrisiken kennen und berücksichtigen, d.h. Wachstumsstrategien gehen Hand in Hand mit Sicherheitsstrategien. Die Verantwortung hierfür liegt nicht allein bei der IT-Abteilung, sondern betrifft die Unternehmensführung.

Alle Entscheider, egal ob Vertrieb, Produktion, Verwaltung oder IT, müssen Prozesse und Strukturen für eine umfassende IT-Sicherheit definieren.

Moderne und erfolgreiche IT-Security-Konzepte zeichnen sich dadurch aus, dass Bedrohungen für das eigene Unternehmen und Geschäftsmodell bekannt sind, realistisch eingeschätzt werden – einschließlich möglicher Konsequenzen – und entsprechende Abwehrmaßnahmen eingesetzt und eingehalten werden. Das betrifft alle Mitarbeiter eines Unternehmens.

Es ist niemals eine Frage des OB, sondern des WANN.

SECURITY ESSENTIALS

Technische Aspekte

Eine Basisabsicherung mit Virenscanner, Firewall und Passwort-Schutz für Geräte ist heute nicht mehr ausreichend. Moderne Sicherheits-Systeme nutzen spezielle Analyseverfahren für die Erkennung und Abwehr von Angriffen, die Verschlüsselung sensibler Daten und die Identifikation der Nutzer.

Organisatorische Aspekte

Zusätzlich zu Regelungen, wer in welchem Umfang auf welche Daten zugreifen darf und wer Zugang zu sensiblen Unternehmensbereichen erhält, sollten für den Krisenfall Notfallszenarien erarbeitet werden, die eine schnelle Reaktion ermöglichen.

Personelle Aspekte

Nur, wenn alle Mitarbeiter Gefahren und die möglichen Risiken kennen, werden sie in der Lage sein, entsprechend zu handeln. Ein speziell geschulter Sicherheitsbeauftragter kann notwendige Maßnahmen anstoßen und kontrollieren.

Rechtlich Aspekte

Vorgaben des Gesetzgebers und nicht zuletzt der Datenschutz verlangen von Unternehmen, ihre Sichheitskonzepte kontinuierlich an die Gegebenheiten anzupassen. Regelmäßige Zertifizierungen helfen, die Sicherheitsstandards im Unternehmen zu überprüfen.

SWS - Hauzenberg
Brünststr. 2
94051 Hauzenberg
Tel.: +49 (0)8586 / 9604 - 0
Fax: +49 (0)8586 / 9604 - 99

SWS - Regensburg
Im Gewerbepark D75
93059 Regensburg
Tel.: +49 (0)941 / 20605 - 0
Fax: +49 (0)941 / 20605 - 99

SWS - Nürnberg
Nordostpark 16
90411 Nürnberg
Tel.: +49 (0)911 / 148862 - 0
Fax: +49 (0)911 / 148862 - 99

cisco Gold Partner

info@sws.de | www.sws.de