Top-down statt Bottom-up: Cybersecurity muss Chefsache sein

02-11-20 | München | Giesecke+Devrient

Eine durchgängige IT-Sicherheitsstrategie gewinnt gerade in der aktuellen Corona-Pandemie an Bedeutung. Die beschleunigte Digitalisierung fast aller Lebensbereiche hat die Angriffsfläche für Hacker signifikant vergrößert. Mit isolierten Bottom-up-Projekten ist eine umfassende hohe Sicherheit angesichts der komplexen Gefahrenlage kaum zu etablieren, meint Giesecke+Devrient (G+D). Erforderlich ist vielmehr ein ganzheitlicher Top-down-Ansatz. Cybersecurity muss zur Chefsache werden.

Cyberangriffe gewinnen immer mehr an Komplexität und Professionalität. Gleichzeitig steigt die IT-Abhängigkeit von Unternehmen, Behörden und Privatpersonen. Durch die verstärkte Nutzung von Cloud Services und neue Entwicklungen wie Smart City oder Smart Home wird das Gefährdungspotenzial noch einmal drastisch steigen.

Die Gefahrenlage durch Internetkriminelle ist hoch und wird hoch bleiben. In der aktuellen Sonderauswertung „Cybercrime in Zeiten der Corona-Pandemie“ des Bundeskriminalamts heißt es: „Aufgrund des weiter bestehenden Gefahrenpotenzials der Pandemie für Staat und Gesellschaft und der anhaltenden Verschiebungen diverser Lebensbereiche in den virtuellen Raum wird die thematische Bedrohungslage im Cyberbereich als andauernd hoch eingestuft.“ (1)

In den letzten Jahren haben Unternehmen verstärkt in IT-Security investiert. Trotz aller Anstrengungen bestehen aber weiterhin großen Herausforderungen, die eine Erweiterung der bestehenden Sicherheitskonzepte erfordern. Laut Bitkom liegt der Gesamtschaden für die deutsche Wirtschaft in den Jahren 2018 und 2019, der durch Datendiebstahl, Sabotage oder Spionage entstand, bei jeweils mehr als 100 Milliarden Euro – Tendenz steigend (2).

Bemühungen der Unternehmen sind oft auch deshalb nicht ausreichend, weil häufig singuläre Sicherheitsmaßnahmen von einzelnen Bereichen umgesetzt werden, so dass IT-Sicherheitssilos entstehen. Mit solchen Insellösungen, die nur ein bestimmtes Sicherheitsthema adressieren – etwa den Perimeterschutz oder applikationsbezogene Maßnahmen – kann keine durchgängig hohe Sicherheit realisiert werden. Dieser Bottom-up-Ansatz ist nicht zielführend. Deshalb drängen IT-Sicherheitsexperten schon lange darauf, dass sich die Chefetage dem Problem ganzheitlich annimmt.

Es muss eine umfassende IT-Sicherheitsstrategie entwickelt, etabliert und konsequent umgesetzt werden. IT-Sicherheit sollte zudem als ein integraler Bestandteil der Unternehmensstrategie betrachtet werden, und hier ist im Sinne eines Top-down-Ansatzes die Management-Ebene gefordert. Sie allein kann eine übergeordnete, nachhaltige Sicherheitsstrategie etablieren, Prioritäten setzen, erforderliche Strukturen schaffen und notwendige Budgets bereitstellen.

Die Führungsebene muss also der Initiator einer unternehmensweiten Sicherheitsstrategie und -kultur sein, aber selbstverständlich muss eine solche Kultur auch gelebt werden. Folglich ist der Faktor Mensch, sprich der einzelne Mitarbeiter, ebenfalls von entscheidender Bedeutung.

Auch bei der besten Strategie und Nutzung neuester Sicherheitstechnologien und -lösungen bleibt der einzelne Mitarbeiter ein potenzielles Einfallstor beispielsweise für Phishing-Mails und Social Engineering, wenn das Bewusstsein für Cyberangriffe und -sicherheit fehlt. Die Sensibilisierung der Mitarbeiter für Sicherheitsgefahren, Schulungen und die Vermittlung von Best Practices für den sicheren Umgang mit Informationstechnologie sind deshalb unverzichtbare Maßnahmen bei der Umsetzung einer unternehmensweiten Sicherheitsstrategie. Es muss also eine Denkweise für Cybersicherheit entstehen, die tief im Bewusstsein aller Beschäftigten eines Unternehmens verankert ist.

„Gerade in dieser Zeit ist Cybersicherheit der entscheidende Erfolgsfaktor für die weitere Digitalisierung. Deshalb müssen wir sowohl das Bewusstsein dafür erhöhen als auch unsere Investitionen in IT-Sicherheit und entsprechende Infrastrukturen steigern“, erläutert Ralf Wintergerst, Vorsitzender der Geschäftsführung und Group CEO von Giesecke+Devrient. „Auf Unternehmensseite fallen beide Aufgaben klar in den Verantwortungsbereich des Top-Managements.“

„Und dabei darf ein wesentlicher Punkt nicht übersehen werden“, so Wintergerst weiter, „wir sollten IT-Sicherheit als eine Chance betrachten und nicht als notwendiges Übel. Denn: Die Sicherheit der Netze und der Kommunikationsinfrastrukturen ist wichtiger denn je.“

(1) vgl.: Cybercrime Sonderauswertung Corona 2019

(2) vgl.: bitkom Studie Wirtschaftsschutz 2020

Über Giesecke+Devrient

Giesecke+Devrient (G+D) ist ein weltweit tätiger Konzern für Sicherheitstechnologie mit Hauptsitz in München. Innovationen von G+D machen das Leben von Milliarden von Menschen in der digitalen und physischen Welt sicherer. In den Bereichen Bezahlen, Konnektivität, Identitäten und Digitale Infrastrukturen gehört G+D mit seinen Produkten und Lösungen zu den Markt- und Technologieführern.

Das 1852 gegründete Unternehmen erwirtschaftete im Geschäftsjahr 2019 mit 11.500 Mitarbeiterinnen und Mitarbeitern einen Umsatz von 2,45 Milliarden Euro. G+D ist in 33 Ländern präsent. Zu den Kunden zählen unter anderem Zentral- und Geschäftsbanken, Mobilfunkanbieter, Automobilhersteller, Krankenkassen sowie Regierungen und Behörden. Weitere Informationen: www.gi-de.com.