EINE PUBLIKATION DES REFLEX VERLAGES ZUM THEMA

JUNI 2020

IT-Sicherheit

So impfen Sie Ihre Systeme

PRESSECLIPPING IS4IT

www.it-sicherheit-info.de

REFLEX Verlag

GRUSSWORT

Aufräumen und zukunftssicher Aufstellen

Viele Unternehmen kämpfen um ihr Überleben. Manche müssen zugeben, dass es niemals eine Risikobetrachtung gegeben hat, wie auf ein Ereignis zu reagieren wäre, das über Nacht alle Prozesse lahmlegt. Die Corona-Krise ist noch lange nicht vorbei. Aber IT-Sicherheitsverantwortliche arbeiten daran, ihre Organisation in den geregelten Betrieb zurückzuführen. An vielen Stellen wird deutlich, welche Mühen die Aufräumarbeiten machen, bis Arbeitsprozesse anlaufen. Parallel zu den Aufräumarbeiten ist es höchste Zeit für die Ausarbeitung von Notfallplänen und detaillierte Diskussionen von Szenarien und Schutzmechanismen. Denn bei der nächsten Krise sollen digitalisierte und automatisierte Systeme bereitstehen, damit Roboter und künstliche Intelligenzen ihren Teil dazu beitragen, die Arbeitsprozesse am Laufen zu halten und die Wirtschaft zu schützen.

Christian Raum
Chefredakteur

Partner

ALLGEIER IT

team2work

RAPID7

Das Papier der Publikation, die im aufgeführten Trägermedium erschienen ist, stammt aus verantwortungsvollen Quellen.

B.A.U.M.

„Deutschland ist im Homeoffice-Modus"

Dr. Holger Mühlbauer, Geschäftsführer des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) berichtet im Interview, welche IT-Sicherheitsvorkehrungen Nutzer in ihrem Homeoffice umsetzen. Der Verband sieht einen „Digitalisierungsschub", der jetzt mit mehr Bewusstsein für IT-Sicherheit verbunden werden muss. Hierfür bietet die IT-Sicherheitsbranche kostenfrei Unterstützung und Beratung bei der sicheren Anbindung von Arbeitsplätzen außerhalb des Unternehmens an.

Wie haben die Unternehmen aus Ihrer Sicht auf die Corona-Krise reagiert? Viele IT-Verantwortliche reagieren mit einer enormen Beschleunigung der Digitalisierung. Erzwungenermaßen haben sie in kurzer Zeit Homeoffice-Arbeitsplätze eingerichtet. Die Intention war es, Betriebsstrukturen und Arbeitsprozesse aufrechtzuerhalten. Doch nicht jedes Unternehmen verfügt über die IT-Infrastruktur, um das Homeoffice der Mitarbeiter adäquat zu sichern. Das bereitet uns Sorgen.

An welchen Beobachtungen machen Sie das fest? In etlichen Fällen werden hilfsweise private Hard- und Software sowie Netzanbindungen genutzt. Möglicherweise sind auch nicht alle Komponenten, die Unternehmen und Organisationen ad hoc zur Verfügung stellen, in Bezug auf IT-Sicherheit auf dem aktuellen Stand der Technik.

Welche Risiken sehen Sie in der aktuellen Situation? Die derzeitige flächendeckende Umstellung auf mobiles Arbeiten, Homeoffice, Datenübermittlung und Remote-Authentifizierung stellt erhöhte Anforderungen an die IT-Sicherheit. Wir haben eine Liste mit zehn empfohlenen Sicherheitsvorkehrungen erstellt. Um einen Überblick zu bekommen, haben wir in einer deutschlandweiten Umfrage ermitteln lassen, welche dieser Vorkehrungen die Homeoffice-Nutzer anwenden. Die am häufigsten genannten Funktionen sind:

- 65 Prozent der Mitarbeiter nutzen sichere Passwörter für ihren Rechner im Homeoffice.
- 63 Prozent der Befragten haben ihr WLAN mit einem Passwort geschützt.
- In 61 Prozent der Homeoffices sind Virenschutzprogramme installiert.

Zu welchen Schlüssen kommen Sie bei der Analyse dieser Zahlen? Das Ergebnis zeigt, dass durchaus Problembewusstsein für IT-Sicherheit besteht. Allerdings sehen wir bei allen von uns vorgeschlagenen Sicherheitsfunktionen auch einen erheblichen Überzeugungsbedarf. Über eine öffentliche Webseite stellen unsere Mitglieder deshalb für drei Monate kostenfreie IT-Sicherheitslösungen einschließlich Fernberatung zur Verfügung. Die Angebote richten sich an alle betroffenen Anwender.

Wir hoffen, dass es uns gelingt, den jetzt erkennbaren Bewusstseinswandel für Sicherheitsprobleme und Digitalisierungsvorhaben mit einem angemessenen Maß an IT-Sicherheit zu verbinden. Damit bewirken wir in der aktuelle Situation hoffentlich etwas Positives.

„Anwender fordern detaillierte Analysen"

Ronny Schubhart, Bereichsleiter IT-Security bei IS4IT erklärt, wie eine intelligente Monitoringlösung wie IBM QRadar bei der präzisen Analyse von Sicherheitsbedrohungen unterstützt und so der Entscheidungsfindung in Sicherheitsteams und im Management dient.

Welches ist das wichtigste Kriterium bei der Auswahl einer IT-Sicherheitslösung? Die IT-Sicherheit ist in den allermeisten Fällen nicht der Geschäftszweck eines Unternehmens. Hier wird IT-Sicherheit nicht eingesetzt, weil sie einen Vorteil auf dem Markt verschaffen würde, sondern weil die Reputation und das Überleben der Organisation in Frage steht. Deshalb sollten Unternehmen genau prüfen, ob es die richtige Entscheidung sein kann, diese Sicherheit selbst herzustellen oder sich auf einen Dienstleister zu verlassen.

Welche Argumente sprechen aus Ihrer Sicht für die Arbeit mit einem Dienstleister? Zu den Aufgaben des Dienstleisters zählt es, Sicherheit objektivierbar zu machen. Hierfür gibt es feste Regeln, Gesetze, Zertifizierungen, die auch in Audits geprüft werden. Die gesamte Klaviatur dieser möglichen Schutzmechanismen wird sicher von keiner Organisation gespielt werden. Vielmehr ist es die Entscheidung des Managements, wie viele Funktionen in Anspruch genommen werden – und welche Risiken als kalkulierbar erscheinen. Klar ist, der Anwender kann diese Leistung von seinem Provider fordern: Risiken zeigen, Risiken analysieren, Risiken bewerten, um auf Basis dieser Berichte die richtigen Entscheidungen zu treffen. Im Kern der Systeme der Dienstleister arbeitet eine intelligente Software, deren Aufgabe ist es, aus riesigen Datenmengen die Analysen zu erstellen, aus denen Sicherheitsanbieter im nächsten Schritt Empfehlungen für ihre Kunden ableiten.

Welche Bedeutung haben Wirtschaftlichkeitsanalysen wie „Return on Investment" oder „Total Cost of Ownership"? Die sind natürlich fundamental. Denn die Verantwortlichen eines Unternehmens müssen Sicherheit berechnen können, um fundierte Entscheidungen treffen zu können. Diese sind immer die Abwägung eines bestimmten Risikos mit den entstehenden Kosten – und an dieser Stelle spielen auch operative Kriterien eine wesentliche Rolle. Die Analysen zeigen auch, ob es für ein Unternehmen günstiger ist, die IT-Sicherheit mit einem eigenen Team zu erzielen oder ob sich das Management auf einen externen Dienstleister verlassen sollte.

Welche Rolle spielt dabei die intelligente Software als Kern eines Sicherheitssystems? Es ist die zentrale Instanz für Bewertungen, Korrelationen, Analysen, Empfehlungen innerhalb einer Infrastruktur. Hierzu beobachtet und analysiert das System das Nutzerverhalten. Diese Auswertungen werden vom System aufbereitet und an die Sicherheitsteams zur Bearbeitung weitergegeben. Sie sind auch Grundlage für die Kosten-Nutzen-Rechnung.