DEUTSCHER MITTELSTANDS-BUND

Digitalisierung	Arbeit & Bildung	Energiewende	Finanzen

Interview mit Peter Lachenmair, IT Security Experte

„Das Home-Office ist als neue Verteidigungszone hinzugekommen“

Themenwoche: Cybersecurity im Mittelstand

06. Mai 2021

Kontakt zur Redaktion:
Deutscher Mittelstands-Bund (DMB) e.V.
Grafenberger Allee 125
40237 Düsseldorf

www.mittelstandsbund.de
Tel. +49 (0) 211 / 2005 25-0
Fax +49 (0) 211 / 2005 25-99
Mail: info@mittelstandsbund.de

Herausgeber (V.i.S.d.P.):
Marc S. Tenbieg
Geschäftsführender Vorstand
meinung@mittelstandsbund.de

Peter Lachenmair[1]

„Das Home-Office ist als neue Verteidigungszone hinzugekommen“

Themenwoche: Cybersecurity im Mittelstand

Neue Angriffsflächen, mangelnde Risikoeinschätzung und fehlende Sensibilisierung unter mittelständischen Unternehmen. Der DMB hat mit Cybersecurity-Experte Peter Lachenmair über die Gefahren und Herausforderungen der Cyberkriminalität gesprochen. Was können kleine und mittlere Unternehmen kostengünstig umsetzen? Welche Services werden die künftigen Entwicklungen bestimmen? Und warum tun sich KMU mit dem Thema Cybersecurity allgemein so schwer?

DMB: Herr Lachenmair, das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat kürzlich in einer repräsentativen Umfrage herausgefunden, dass mobiles Arbeiten und Home-Office die Angriffsfläche für Cyber-Kriminelle stark vergrößert hat. Warum ist das so?

Lachenmair: Das Home-Office ist insbesondere durch Corona als neue „Verteidigungszone“ hinzugekommen. Das hat nicht zwangsläufig etwas mit der Hardware zu tun. Das Home-Office ist eben, wenn man so will, ein quasi öffentlicher Raum, auf den verschiedene Personen Zugriff haben. Die Konzentration der Mitarbeiter ist zudem im Home-Office geringer. Ablenkungen können beispielweise die Ursache dafür sein, dass eine E-Mail mit Schadsoftware angeklickt wird. Das Bewusstsein beziehungsweise die Awareness für Sicherheit ist nach einem Jahr im Home-Office oft nicht so stark ausgeprägt wie im Büroumfeld. Ein weiterer Faktor ist die Tatsache, dass sämtliche Sicherheits-Parameter sehr schnell geöffnet wurden. Von einem Tag auf den anderen stand der Auszug aus der Büroumgebung ins Home-Office an. Dabei wurden die Firewalls schnell aufgebohrt und Virtual Private Networks (VPN) notdürftig eingerichtet. Auch die IT befindet sich seit einem Jahr im Ausnahmezustand. Die Kapazitäten reichen in vielen Unternehmen maximal für die Aufrechterhaltung des Betriebs, aber nicht für die gesamte Wartung.

Was sind aus Ihrer Erfahrung die wesentlichen Herausforderungen für KMU in Bezug auf Cybersecurity?

Die Aufrechterhaltung der Awareness, also des Problembewusstseins, für das Thema Cybersecurity. Mitarbeiter*innen sollte die Bedrohungslage durch regelmäßige

[1] Peter Faxe Lachenmair ist Peter „Faxe“ Lachenmair ist seit mehr als 20 Jahren als IT-Berater für mittelständische Unternehmen und Konzerne aktiv. Der Fokus seines Unternehmens Lachenmair IT-Consulting liegt auf Informationssicherheit und IT-Security. Als Information Security Architect beschreibt er Sicherheitskonzepte für Unternehmen. Als Cyber Security Awareness Mentor analyisiert er den Status-Quo, weckt Bewusstsein für die Bedrohungslage und schafft Lösungskompetenz im Unternehmen.

Schulungsmaßnahmen regelmäßig vor Augen geführt werden. Auch der Einsatz von Security-Tests im Rahmen einer Awareness-Kampagne ist denkbar. Dabei ließe sich zum Beispiel herausfinden, wie viele Nutzer*innen tatsächlich unbewusst Phishing-Mails anklicken. Diese Ergebnisse können dann für weitere Schulungsmaßnahmen genutzt werden. Dabei sollte nicht die Rüge, sondern stets der Trainingseffekt im Vordergrund stehen. Wie kann ich beispielsweise Malware erkennen? In KMU fehlt leider die Wahrnehmung, dass das ein kritisches Thema ist. Dabei erfolgen viele Angriffe immer noch über die klassischen Wege wie zum Beispiel E-Mails und es wäre recht einfach, Mitarbeiter*innen dahingehend zu sensibilisieren.

Seit Jahren ist ein Trend erkennbar: Insbesondere kleine und mittlere Unternehmen werden Opfer von Cyberattacken. Woran liegt das?

Der durchschnittliche Mittelständler geht nach wie vor davon aus, dass Cyber-Kriminelle kein interessantes und wertvolles Diebesgut in kleinen und mittleren Unternehmen finden. Vor dem Hintergrund einer “Supply-Chain-Attack" (ein Cyberangriff auf die Lieferkette; *Anm. D. Redaktion*) ist jedoch ein Mittelständler mit 20 Mitarbeiter*innen genau so interessant wie ein Großkonzern, wenn das mittelständische Unternehmen für einen großen Hersteller ein einzelnes Sonderteil produziert. Alle Unternehmen sind letztendlich Zulieferer für ein nächstgrößeres Unternehmen. Da die kleineren Unternehmen in der Regel schlechter geschützt sind, wird diese Schwachstelle häufig als Eintrittspunkt genommen, um die großen Netzwerke anzugreifen. Die kleinen Unternehmen sind dann tatsächlich die Brückenpunkte, um weitere Angriffe durchzuführen.

Der Grund liegt darin, dass IT schlichtweg Geld kostet und bei vielen KMU noch nicht den notwendigen Stellenwert in der Priorisierung hat. Nehmen wir ein Mittelstandsunternehmen mit 50 Mitarbeitern. Die Kosten, die für einen IT-Spezialisten erwirtschaftet werden müssen, lasten dann auf den Schultern dieser 50 Mitarbeiter. Bei 500 Mitarbeitern sind die Kosten, die jeder einzelne erwirtschaften muss, geringer. Das heißt für die kleineren Unternehmen, dass neue Modelle entwickelt werden müssen, um Sicherheitsstandards dennoch erhöhen zu können. Gleichzeitig muss vermieden werden, dass sich das Unternehmen in einer Kostenfalle verliert.

Welche unternehmerische Priorität räumen KMU erfahrungsgemäß dem Thema Cybersecurity ein?

Im Risikomanagement gibt es die Begriffe “Risikoappetit” und “Risikoabschätzung”. Aufgrund des fehlenden Wissens ist die Risikoabschätzung für Cybersecurity-Themen eher niedrig und dadurch wächst ein größerer Risikoappetit. Manche Unternehmen ändern auch dann wenig, wenn sie tatsächlich bereits angegriffen wurden. Für andere stellt sich ein Cyberangriff genau so drastisch dar wie ein Brand des Betriebsgebäudes. Viele Unternehmen fangen erst dann an zu investieren, wenn sie betroffen sind. Genau hier liegt das Problem. Es braucht mehr Bewusstsein für diese Themen und mehr Prävention. Die Bereitschaft, Risiken einzugehen, indem man das Thema Cybersecurity vernachlässigt, ist leider groß. Die Unternehmen müssen sich darüber bewusster werden, dass eine solche vermeintlich immaterielle und von daher unwirklich erscheinen Bedrohung tatsächlich besteht. Wenn das Haus bereits abgebrannt ist, ist es leider schon zu spät. Es ist darüber hinaus eine Frage des Renommees. Wenn bekannt

wird, dass ein mittelständischer Maschinenbauer, der größeren Unternehmen zuliefert, gehackt wurde, wird dieser Zulieferer möglicherweise früher oder später ausgetauscht. Auch die größeren Unternehmen schauen sich ihre Zulieferer genauestens an und erwarten hohe Qualität und entsprechende Sicherheitsstandards. Ein gutes Beispiel ist die TISAX Zertifizierung in der Automobilindustrie. Sollte ein mittelständischer Zulieferer gehackt werden, wird es in der Tat mit der Folgezertifizierung schwer.

Cybersecurity bedeutet für viele mittelständische Unternehmen Komplexität, hohe Kosten und fehlende Expertise. Was sind kostengünstige und einfach umsetzbare Sicherheitsmaßnahmen?

Das Thema "Managed Services" wäre ein guter Ansatzpunkt, um das Sicherheitslevel im Unternehmen zu erhöhen. Über einen Dienstleister werden verschiedene IT-Leistungen eingekauft und so das Schutzlevel im Unternehmen erhöht. Beispiele sind Firewalls oder Virenschutzscanner. Diese kommunizieren mit dem spezialisierten Dienstleister und bieten dadurch eine erhöhte Schutzstufe. Ähnliche Trends gibt es im Bereich des Patch-Management, wo es darum geht, dass die Maschinen immer auf dem aktuellen Stand sind. Mit dem Dienstleister können auch weitere Einsatzmöglichkeiten identifiziert und definiert werden. Es gibt Services, bei denen der Dienstleister letztendlich das gesamte Rechenzentrum zur Verfügung stellt und beaufsichtigt. Der Unternehmer muss dann nur noch seine Fachapplikationen installieren. So wird der Kontrollbereich recht eng gehalten und kann selbst mit einem vergleichsweise kleinen internen Personalsockel bedient werden.

Welcher Faktor spielt der IT-Fachkräftemangel für das Thema Cybersecurity?

Ich gehe davon aus, dass in den nächsten ein bis zwei Jahren die Berufsschulung des „Cybersecurity-Spezialisten" angeboten wird. So nüchtern es auch klingen mag, wir werden dadurch in den nächsten vier Jahren eine Schwemme von geringqualifizierten Cybersecurity-Spezialisten haben, die der Markt dann nach fünf bis sechs Jahren wieder ausspuckt. Das ist eine Erfahrung, die sich in den letzten zwanzig Jahren häufiger gezeigt hat. Das bedeutet, dass es nicht wesentlich mehr gute Spezialisten geben wird. Diese werden weiterhin für IT-Dienstleistungsunternehmen, große Konzerne und Beratungshäuser arbeiten. Sie sind in der Regel zu teuer für ein mittelständisches Unternehmen.

Daher erleben wir bereits heute die Entwicklung, dass man sich für die Nachwirkungen eines Cyberangriffs wappnet, etwa durch die Absicherung über eine Cyberschutz-Versicherung. Zudem braucht es Hilfestellungen und preislich akzeptable Beratungsangebote für Unternehmen. Insbesondere dann, wenn es zu einer Cyberattacke gekommen ist und es darum geht, die Situation schnell wieder in den Griff zu bekommen. Fehlen die entsprechenden Experten im eigenen Unternehmen, sind Wartungsmodelle unter Einbeziehung eines externen Spezialisten für eine gewisse Stundenanzahl im Jahr eine gute Option. So hat der mittelständische Unternehmer eine gewisse Kalkulationssicherheit. Ich gehe davon aus, dass solche Modelle in Zukunft stärker nachgefragt werden.

Wie können sich kleine und mittlere Unternehmen besser vor Cyber-Attacken schützen? Gibt es kostengünstige und leicht umsetzbare Ansatzpunkte?

Es gibt in der Tat mehrere Ansatzpunkte, wie man den Schutzlevel ohne viel Aufwand unmittelbar erhöhen kann. Erstens, eine Fritzbox ist keine Firewall. Nutzen Sie eine Business Firewall. Zweitens, kostenfreier Antivirus-Schutz bringt nichts. Drittens, E-Mails aufmerksam lesen, bei Unsicherheit einmal tief durchatmen und dann noch einmal lesen. Das sind drei ganz simple Punkte, wie Unternehmer*innen Angriffsflächen unmittelbar reduzieren können. Ich will den letzten Punkt mit den E-Mails aber noch einmal hervorheben. Man kann sich da mit einer einfachen Regel absichern und sollte sich immer die folgenden Fragen stellen. Erwarte ich tatsächlich eine E-Mail von dem Absender? Betrifft der Betreff der E-Mail tatsächlich mich selbst? Und sieht die E-Mail so aus, wie sie immer aussieht? Auf diese Weise lässt sich die Gefahr durch Phishing-Nachrichten erheblich reduzieren. Vor Fehlern ist niemand sicher, aber alleine durch aufmerksames Lesen kann man die Fehlerquote erheblich reduzieren.

Vielen Dank für das Gespräch!