Steffen Mai: 5 Tipps, mit denen mittelständische Unternehmen sich wirksam vor Cyberangriffen schützen

Steffen Mai · **Bildrechte**: 3 Plus Solutions GmbH & Co. KGi · **Fotograf**: 3 Plus Solutions GmbH & Co. KG

Digitalisierung ist heutzutage unerlässlich, um als mittelständisches Unternehmen wettbewerbsfähig zu bleiben. In diesem Zusammenhang bietet das Team der 3 Plus Solutions GmbH & Co. KG ein bislang einzigartiges Konzept, um Unternehmer ganzheitlich zu unterstützen. Im Folgenden erfahren Sie, wie sich mittelständische Firmen optimal gegen digitale Bedrohungen absichern und im Ernstfall handlungsfähig bleiben.

Die Gefahr durch Cyberangriffe wächst täglich: Allein im Jahr 2022 kam es in Deutschland zu Schäden in Höhe von 203 Milliarden Euro, wie Bitkom berichtet. Dabei trifft es längst nicht mehr nur die ganz Großen - gerade kleine und mittlere Unternehmen sind oft schlecht auf Cyberangriffe vorbereitet und werden so zum gefundenen Fressen für Hacker. „Oftmals glauben mittelständische Unternehmen, sie seien zu uninteressant für Angreifer oder die nötigen Schutzmaßnahmen seien zu teuer und aufwendig. Dieser Fehler rächt sich allerdings, wenn tatsächlich einmal etwas passiert“, warnt Steffen Mai, Geschäftsführer der 3 Plus Solutions GmbH & Co. KG.

„Die meisten Hacker machen schließlich keinen Unterschied zwischen großen und kleinen Firmen“, so der IT-Experte weiter. „Um ihnen gar nicht erst ausreichend Angriffsfläche zu bieten, müssen Unternehmen sich auf technischer Ebene bestmöglich schützen und ihr Personal für die Bedrohung durch Cyberangriffe sensibilisieren.“ Als Geschäftsführer der 3 Plus Solutions GmbH & Co. KG unterstützt Steffen Mai gemeinsam mit seinem Geschäftspartner Marco Schröder Unternehmer seit mehr als zehn Jahren dabei, sich rundum bestens für die zunehmend digitalisierte Geschäftswelt aufzustellen. Während Marco Schröder als Marketingexperte vor allem kleinere und mittlere Unternehmen beim Markenaufbau unterstützt und so das Personal-Recruiting und die Neukundengewinnung sowie letztlich auch die Umsatzsteigerung unterstützt ist Steffen Mai als IT-Experte ist Steffen Mai in erster Linie für das firmeninterne IT-Systemhaus verantwortlich, das die Geschäftsführer seit 2013 gemeinsam betreiben und Kunden bei sämtlichen Angelegenheiten rund um die IT im Unternehmen betreut. Was Unternehmen tun sollten, um sich gegen Cyberangriffe zu schützen, hat Steffen Mai im Folgenden zusammengefasst.

1. Redundante, isolierte Backups anlegen

Bei einem Angriff oder Systemausfall ist eine der größten Sorgen der Verlust wichtiger Daten. Damit dies im Notfall nicht geschieht, sollten Unternehmen redundante Backups wichtiger Daten auf separaten Medien erstellen. Im Klartext bedeutet das, Kopien geschäftsrelevanter Daten an verschiedenen Orten abzuspeichern, die nicht zum selben lokalen Netzwerk gehören - zum Beispiel in unterschiedlichen Rechenzentren.

Werden regelmäßig Backups aller wichtigen Daten erstellt und extern gesichert, liegt bei einem Ausfall oder Cyberangriff ein Abbild vor, das zur Wiederherstellung genutzt werden kann. Dadurch ist es dem Unternehmen möglich, seine Handlungsfähigkeit schneller zurückzuerlangen.

2. Systeme überwachen und auf dem neuesten Stand halten

In der IT ist es zudem von entscheidender Bedeutung, frühzeitig zu handeln und Schwachstellen zu schließen, bevor sie zum Problem werden. Unternehmen sollten daher ihre Systeme und ihr Netzwerk kontinuierlich mit geeigneten Tools überwachen, die sie auf Auffälligkeiten hinweisen.

Darüber hinaus ist ein effizientes Update-Management unverzichtbar. Indem ein Unternehmen sämtliche verwendeten Anwendungen stets auf dem aktuellsten Stand hält, lässt sich ein Großteil der Sicherheitslücken auf Seiten der Software vermeiden. Diese Aufgabe lässt sich ebenfalls zu großen Teilen mittels spezieller Tools für das Update-Management automatisieren.

3. Mitarbeiter auf Bedrohungen vorbereiten

Um Hackerangriffe effektiv zu vereiteln, müssen zunächst die Beschäftigten auf die Risiken vorbereitet werden. Viele Hacker greifen nicht über Schadcode, sondern über sogenanntes Social Engineering an - Angriffe, die Menschen dazu verleiten, Zugangsdaten preiszugeben oder Hackern den Zugriff zu erlauben. Unternehmen sollten daher ihre Mitarbeiter in regelmäßigen Abständen für die aktuellen Maschen sensibilisieren. Dafür hat es sich als effektiv erwiesen, die Gefahren in Schulungen zu besprechen und mit Mitarbeitern zu üben, wie sie einen potenziellen Social-Engineering-Angriff erkennen und darauf reagieren.

Zusätzlich sollten Mitarbeiter mit dem Umgang mit sensiblen Daten vertraut gemacht werden, damit sie nicht versehentlich den Weg für Missbrauch oder Angriffe ebnen. Klare Richtlinien und regelmäßige Schulungen sind dafür unerlässlich. Jeder Mitarbeiter sollte zumindest wissen, welche Daten als sensibel einzustufen sind, wie damit zu verfahren ist und welche Folgen dem Unternehmen bei Zuwiderhandlung drohen.

4. Netzwerke durch Firewalls und Segmentierung schützen

Angriffe über das Unternehmensnetzwerk sind jedoch nicht auszuschließen. Eine aktuelle und verlässliche Firewall hilft dabei, Angreifer abzuwehren. Gibt es verdächtigen Datenverkehr zwischen dem Unternehmensnetzwerk und dem Internet, kann eine Firewall diesen unterbinden und so das Unternehmen schützen. Dafür muss sie jedoch dafür konfiguriert werden, nur autorisierten Datenverkehr zuzulassen.

Ergänzend dazu sollte das Netzwerk mithilfe virtueller lokaler Netzwerke (VLAN) weiter segmentiert werden. Auf diese Weise lassen sich sensible Daten und Systeme effektiv abschotten - Hacker, die Zugriff erlangen, können also nur auf einen kleinen Teil der Daten im Netzwerk zugreifen.

5. Rechtzeitig für Notfälle planen

Sollte es dennoch zu einem IT-Ausfall oder einem ähnlichen Notfall kommen, sind Unternehmen auf einen funktionierenden Notfallplan angewiesen. Es gilt daher, die relevanten Bedrohungen und Risiken im Blick zu behalten und auf dieser Basis Pläne zu erstellen und zu erproben, die bei der Bewältigung von Krisen helfen.

Da sich digitale Bedrohungen ständig weiterentwickeln, müssen die Notfallpläne dies selbstredend auch tun. Unternehmen sollten deshalb regelmäßig prüfen, ob die Notfallpläne noch dazu geeignet sind, aktuelle Bedrohungen zu überwinden. Nur so gelingt es, im Ernstfall schnellstmöglich zum Regelbetrieb zurückzukehren.