ZWEI BILDER, 156 TAGE, 71.000 € UNTERSCHIED

Cybersicherheit im Unternehmen: Bei vielen ist es bereits 5 vor 12 ...

Analoger Einbruch

Einen analogen Einbruch erkennen wir sofort, wenn wir das Unternehmen betreten - alles ist durchwühlt, ein Fenster ist aufgebrochen, Gegenstände oder Geld fehlen. Wir rufen die Polizei und „wissen“, was gemacht werden muss.

Digitaler Einbruch

Wir sehen nichts, keine Einbruchsspuren; niemand war physisch vor Ort. Trotzdem kostet der durchschnittliche Schaden 71.000 €. Es dauert durchschnittlich 156 Tage, bis man bemerkt, dass man gehackt wurde. Wie ist dann das Vorgehen?

Cybersicherheit ist nicht optional

Vor dem Hintergrund der Digitalisierung sind Unternehmen vermehrt der Gefahr ausgesetzt, Opfer von Cyberkriminalität zu werden. Diese Sicherheitsrisiken gilt es zu minimieren: durch technische und organisatorische Lösungen, die Absicherung der Restrisiken durch eine Cyberversicherung und vor allem auch durch Sensibilisierung mithilfe entsprechender Präventionsmaßnahmen und Schulungen.

Befragungen haben ergeben, dass das Thema IT-Sicherheit und IT-Sicherheitsrisiken-Minimierung sowie die Umsetzung der Datenschutzgrundverordnung (DSGVO) von den meisten Unternehmen als das drängendste Problem angesehen wird und sie auf die damit verbundenen Haftungsrisiken nicht vorbereitet sind.

Durch Präventionsmaßnahmen wie Mitarbeiterschulungen und Phishingsimulationen kann für das Thema sensibilisiert und die IT-Sicherheit im Unternehmen gestärkt werden. Die Bereitstellung von Prozesswerkzeugen – auch zum Thema DSGVO - sorgt dafür, im Fall von Cyberbedrohungen vorbereitet zu sein und verhältnismäßig sowie zeitgemäß reagieren zu können. Auch im Hinblick auf die Versicherungsbedingungen einer Cyberversicherung müssen Obliegenheiten eingehalten und Prävention betrieben werden damit im Schadensfall die volle Leistung abgerufen werden kann.

Wir haben in unserem Unternehmen ein Online-Tool, welches Dienste zur Cybersicherheit anbietet, getestet.

„Als die Fake-Phishing-Mail herumgeschickt wurde war niemand darauf vorbereitet. Es haben von 20 Kollegen 3 den Phishing-Link angeklickt. Wäre es kein Fake gewesen, hätte es schon bei nur einem Klick fatale Folgen gehabt... “

– Mark Stegmann
Spezialist Cyberversicherung

Jeder Mitarbeiter bekommt einen persönlichen Zugang. Es werden gezielt Webinare eingestellt, welche ein Grundlagenwissen für IT-Sicherheit schulen. Zudem gibt es ein Notfallmanagement welches in einem Schadenfall viel Zeit spart. Durch regelmäßige interessante News zur Cyberkriminalität wird die Aufmerksamkeit aufrechterhalten und der regelmäßige Versand von Phishing-Mails macht den Erfolg im eigenen Unternehmen messbar. Die Mitarbeiter, die versehentlich den Fake-Phishing-Link angeklickt haben bekommen direkt eine persönliche Meldung und werden entsprechend sensibilisiert. Insgesamt ist die Auswertung anonymisiert, der Administrator sieht nur die Anzahl der Mitarbeiter, die den Fake-Phishing-Link angeklickt haben. Eine Cyber-Security-Plattform wie z.B. „Cyber-Fuchs“ hilft wirklich, Cyberkriminalität zu erkennen und richtig zu reagieren. Die Strategien der Kriminellen werden immer raffinierter; gleichzeitig werden die rechtlichen Anforderungen an Unternehmen erhöht. Es wird zunehmend schwerer ohne Hilfe von einem Profi Herr der Lage zu werden.

Wer wird gehackt?

Jedes Unternehmen in jeder Branche kann ein Opfer werden. Die meisten erfolgreichen Hackerangriffe sind Zufallstreffer. Die Kosten für einen Angriff sind bereits 2020 „explodiert“. Diese haben sich bei kleinen Unternehmen auf durchschnittlich 71.000 € versechsfacht.

Beratung auf Augenhöhe

Von Unternehmer zu Unternehmer:

Mark Stegmann
Spezialist Cyberversicherungen
mark.stegmann@martens-prahl.de
Telefon: + 49 (0) 7424 958 37