Das dunkle Netz … und wie es jeden fesseln kann

Wissen ist Macht – damit einher geht die Tatsache, dass Daten und Informationen ein teures Gut sind. Für einige Bitcoins erhält man im Darknet eine neue Identität, Angriffe auf Unternehmen können eingekauft werden. Das Darknet ist schon lange der Marktplatz für Internetkriminalität.

Katharina Masannek, Fachbereich Cyberversicherungen bei der eurowest Versicherungsmakler GmbH.

Ein Bericht von Katharina Masannek

Das letzte Jahr hat gezeigt, wie schnell sich unsere globalisierte Welt von heute auf morgen verändern kann. Das Coronavirus wurde am 11.03.2020 von der WHO als globale Pandemie eingestuft. Die Folgen waren gravierende Veränderungen in nahezu allen Lebensbereichen: Schulschließungen, Kontaktverbote, Reisebeschränkungen und Home-Office. Unsere Gesellschaft hat sich stark in Richtung der digitalen Welt verlagert – eine gute Gelegenheit für Cyberkriminelle.

Viele Unternehmen mussten innerhalb kürzester Zeit Mitarbeiter und Geschäftsprozessen ins Home-Office verlagern. Das hatte bei vielen zur Folge, dass die IT-Sicherheit zugunsten einer kurzfristig funktionierenden Arbeitswelt bei den Mitarbeitern zu Hause vernachlässigt wurde. Zum Teil wurden private Geräte mitgenutzt, da betriebliche Ressourcen noch nicht vorhanden waren. Gerade kleinere Betriebe, in denen es noch keine Heimarbeitsplätze gab, stellte das vor Herausforderungen.

Nach knapp einem Jahr befinden sich immer noch viele Menschen im Home-Office. Die Unternehmen hatten Zeit, die geschaffenen Lösungen zu überprüfen und zu verbessern. Eine Rückkehr in die „alte Normalität“ ist nicht zu erwarten.

Das BKA hat im September 2020 eine Sonderauswertung zum Thema Cybercrime in der Corona-Pandemie veröffentlicht. Die Behörden haben zunehmend Versuche festgestellt, die gesellschaftliche und wirtschaftliche Notlage auszunutzen. Die hauptsächliche Bedrohung geht laut dieser Auswertung weiterhin von Phishing-Mails und Fake-Webseiten aus.

Das Öffnen einer E-Mail – ein falscher Klick und plötzlich geht nichts mehr. Durch das Öffnen des Anhanges wurde eine Schadsoftware geladen, die sich eigenständig im Netzwerk ausbreitet und zur Verschlüsselung des Systems führt. Sämtliche Daten des Unternehmens (Auftrags- und Kundendaten, Personalunterlagen, Einsatzpläne, etc.) sind nicht mehr abzurufen und der Betrieb steht derweil still.

Die IT-Sicherheit wurde zugunsten einer kurzfristig funktionierenden Arbeitswelt bei den Mitarbeitern zu Hause vernachlässigt

Den Fuhrpark, das Betriebsgebäude und die eigenen Mitarbeiter gut und umfassend versichern – für die Unternehmen eine Selbstverständlichkeit. Doch der Schutz im Kampf gegen Cyberangriffe wird leider zu oft hinten angestellt. Bereits über Präventionsmaßnahmen wie Mitarbeiterschulungen oder ein eindeutiges IT-Sicherheitskonzept im Betrieb lassen sich viele Risiken zwar minimieren, aber nicht ausschließen. Versicherungslösungen nehmen Ihnen dieses „Restrisiko“ ab. Cybercrime schädigt nicht nur die eigene IT-Infrastruktur, wie beispielsweise die beschädigte Hardware, meist ist der Datenverlust das größere Problem. Die Wiederherstellung der Daten und die Information von Betroffenen durch Spezialisten, die durch Versicherungsgesellschaften vorgehalten werden, ist ein unschätzbarer Mehrwert dieser Versicherungslösung, denn die Unternehmen sind im Schadenfall oftmals auf sich alleine gestellt.

Bild: William Potter - shutterstock