IT-Sicherheit in der Immobilienwirtschaft

Heute sind Einzelunternehmen genauso Zielscheibe von Cyberangriffen wie Großunternehmen, denn häufig sind in den kleineren Unternehmen die Sicherheitsmaßnahmen über Jahre hinweg vernachlässigt worden, und Erpressungsversuche versprechen hier Erfolg. Angriffe sind facettenreicher und werden immer komplexer, also müssen ausgefeilte technische und organisatorische Maßnahmen getroffen werden, um sich davor zu schützen – und das auf allen Wegen und Ebenen. Die größten Risiken sind Datenverluste, Lücken in Softwareanwendungen und dem Betriebssystem, Benutzerkennwörter und der Anwender selbst. Diese Punkte und den Endgeräteschutz sowie den Schutz des Netzwerks werden in diesem Beitrag vorgestellt.

○ **von Eric Drissler und Alexander Schäfer**

Datensicherung

Was bedeutet ein Datenverlust in Ihrem Unternehmen? Da es sich mitunter um eine der wichtigsten Ressourcen Ihres Unternehmens handelt, kann ein solcher Datenverlust große finanzielle Folgen mit sich bringen: Sie und Ihre Mitarbeiter können nicht mehr arbeiten, die Kundenzufriedenheit sinkt rapide, entgangener Umsatz und erhöhte, zusätzliche Kosten für die Datenrettung oder Supportdienstleistung (sofern überhaupt möglich) entstehen. Etwaige Vertragsstrafen/Bußgelder sind hierbei noch gar nicht mit betrachtet.

In vielen Unternehmen werden die Datensicherungen entweder gar nicht oder nur in unregelmäßigen Abständen vorgenommen, und die erforderlichen Erfolgskontrollen nach Art. 32 Abs. 1 Buchstaben b, c und d DSGVO finden gar nicht statt. Häufig sieht man in einem solchen Fall erst zu spät, dass eine Sicherung nicht erfolgreich verlief – spätestens dann, wenn versucht wird, Dateien wieder einzuspielen, und dies nicht möglich ist.

Ein weiterer zu betrachtender Aspekt ist das Thema „unverschlüsselte Datenträger". Mittlerweile setzen die meisten Unternehmen auf mobile Endgeräte, wie beispielsweise Notebooks für Geschäftsreisen, und das Arbeiten im Homeoffice. Auch Wechselmedien wie USB-Sticks oder mobile Festplatten sind sehr beliebt. Die Datenträger, die somit auch das Unternehmen verlassen, sind oft unverschlüsselt, und die Gefahr ist sehr hoch, dass hierbei potenziell sensible Daten in falsche Hände gelangen können – sei es durch Diebstahl oder Verlust.

Als Unternehmen sind Sie dazu verpflichtet, die Daten Ihrer Mitarbeiter und Kunden so gut wie nur möglich zu schützen; ein unverschlüsselter Datenträger mit solchen Daten ist als fahrlässig zu werten. Eine Datenträgerverschlüsselung sorgt für die entsprechende Sicherheit, denn die Daten können nicht mehr von Fremden abgegriffen werden. Natürlich gilt dieser Schutz nur so lange, bis jemand das Passwort des Gerätes bzw. der Verschlüsselung kennt.

Risiko durch Lücken in Software, die nicht auf dem aktuellsten Stand ist

Ein funktionierendes Patchmanagement im Unternehmen ist unabdingbar. Alle Systeme müssen mit den neuesten Softwarepaketen versorgt werden. Dies betrifft die Anwendungen ebenso wie das Betriebssystem und die Hardware in Form von Firmware-Updates. Ansonsten besteht das Risiko, dass Ihre Systeme schnell anfällig für Angriffe von außen werden und die Sicherheitsrisiken steigen.

Mit wachsender Anzahl zu verwaltender Systeme wird das Sicherstellen des zeitnahen Einspielens der Aktualisierungen immer komplexer. Hierfür gibt es entsprechende Patchmanagement-Software (z. B. Kaspersky Endpoint Security Advanced oder Avast oder NinjaRMM) die automatisiert nach Lücken und Aktualisierungen der Hersteller suchen und diese dann ausrollen. So werden die Risiken eines Erfolgs

von Cyberattacken minimiert und der Arbeitsalltag entlastet.

Kennwörter

Ein angemessener Zugangs- und Zugriffsschutz in Bezug auf Ihre Systeme muss gewährleistet sein. Wichtig ist nicht nur ein regelmäßiger Wechsel des Kennworts – auch wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) diesen nicht mehr zwingend vorsieht –, sondern auch die Maßnahmen, die Sie im Unternehmen für die Passwörter treffen, z. B. mindestens acht Zeichen, Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen, keine im Wörterbuch enthaltenen Wörter.

So ist es sehr zu empfehlen, unterschiedliche Kennwörter für verschiedene Systeme zu verwenden sowie auf klassische Passwörter, die leicht zu erraten sind, wie beispielsweise Haustiere, Namen von Kindern usw., zu verzichten. Eine Weitergabe persönlicher Passwörter an Dritte ist grundsätzlich zu unterlassen.

Nicht ratsam in Bezug auf einen etwaigen Aufbewahrungsort der Passwörter ist es, Papierzettel am Arbeitsplatz zu deponieren. So haben potenzielle Angreifer leichtes Spiel, und es kann kein Schutz der Systeme mehr gewährleistet werden. Geeignete Passwortmanager (z. B. Kaspersky Passwortmanager, „KeePass") helfen, den Überblick zu behalten, und sorgen für eine sichere Lagerung.

Awareness

Die Schwachstelle im Bereich der Awareness (Bewusstsein) ist der Mensch selbst: Einer der führenden Hersteller für IT-Sicherheitslösungen gibt an, dass 46 % der Cybersicherheitsvorfälle sich auf das Fehlverhalten von Mitarbeitern zurückführen lassen, z. B. schwache Passwörter, Passwortweitergabe, gleiche Passwörter für unterschiedliche Anwendungen, Öffnen von unbekannten Anhängen (E-Mail), Installation und Ausführen von Software aus dem Internet, die Schadcode enthält, sensible Daten als unverschlüsselte E-Mail versenden, Nutzung von häufig unsicheren und kostenfreien Internetdiensten.

Aus diesen und weiteren Gründen ist es empfehlenswert, wenn Mitarbeiter regelmäßig durch Trainings sensibilisiert werden. So fördern Sie Ihre Mitarbeiter bezüglich der umfassenden und praktischen Kenntnisse zur Cybersicherheit. Grundlage hierfür ist die sogenannte „Ebbinghaus'sche Vergessenskurve", die mittels regelmäßiger Wiederholungen (Mircolearning) langfristig dazu führt, dass erlernte Fähigkeiten nicht so schnell vergessen werden. Genau diesen Ansatz verfolgen Awareness-Lösungen, die die Mitarbeiter in beispielsweise zehn Minuten jede Woche durcharbeiten.

Der Ansatz hierfür ist schnell zusammengefasst: Statt mit strengen internen Regularien oder Strafen zu drohen, sollten Unternehmen einfach den Kooperationswillen fördern. Cybersicherheit ist nicht nur eine Frage der Technologie, sondern auch eine Frage der Unternehmenskultur.

Durch diese Form von Awareness trägt jedes Unternehmen dazu bei, dass sich das Bewusstsein der Mitarbeiter für Datensicherheit und Datenschutz deutlich steigert und die Mitarbeiter sich konform verhalten.

Endpoint-Schutz

Was versteht man eigentlich unter einem guten Endpoint-Schutz? Kernziel hierbei ist in jedem Fall, die Endgeräte wie PCs, Laptops, Smartphones – sogenannte Endpoints – in einer IT-Umgebung vor Gefahren zu schützen. Eine Software für Endpoint Protection besitzt in der Regel Funktionen zum Schutz vor Viren, Spyware, Malware und Phishing. Zusätzlich können Firewall-Funktionen integriert sein.

In vielen Unternehmen werden meist nur rudimentäre Funktionen kostenfreier Lösungen eingesetzt. Die Vorteile der Nutzung einer kostenpflichtigen Software sind, dass kommerzielle Scanner zusätzliche Schutzmechanismen wie Webfilter, Next-Gen-Technologien („Next Generation" bedeutet, dass die Systeme eigenständig lernen und mehr Intelligenz bekommen, um auf unbekannte Gefahren schneller reagieren zu können) und eine schnelle Weiterentwicklung bieten. Zudem enthalten sie meist eine Verhaltenserkennung, die als letzte Verteidigungsinstanz abblocken soll, was den Signaturen und der Heuristik entgangen ist.

Viele Programme greifen zudem auf Malware-Informationen aus großen Datenbanken zurück. Hierfür senden sie Prüfsummen von Dateien an den zentralen Server

des Herstellers, um noch schneller auf Bedrohungen und auch bei „False Positives" (gute Dateien oder Anwendungen werden als Schadcode erkannt) reagieren zu können. Diese gesamte Kombination der breiten Verteidigungslinie soll verhindern, dass Malware über eine Schwachstelle in das System eindringt und sich von dort aus im Unternehmensnetzwerk verbreitet.

Einen zusätzlich sehr effektiven Schutz stellt die Applikationskontrolle dar. Darunter versteht man die Überwachung installierter und freigegebener Anwendungen auf Geräten gemäß vordefinierten Richtlinien. Sie funktioniert mittels einer sogenannten Whitelist, die vermerkt, welche Anwendungen bekannt sind und ausgeführt werden dürfen. Alle anderen werden geblockt, und weder die Mitarbeiter noch die Angreifer können diese ausführen.

Firewall

Eine aktive Firewall, die heute als Unified Threat Management (UTM) bezeichnet wird, sorgt direkt am Übergang zwischen dem lokalen Netzwerk und dem Internet für geeignete Sicherheit. Sie ist vergleichbar mit einer Sicherheitstür und Türstehern, die Passanten überprüfen. Eingehende Datenpakete werden inhaltlich geprüft und Angriffe direkt abgewehrt.

Auch bieten moderne UTM-Lösungen Funktionen wie die Verschlüsselung von ausgewählten ausgehenden E-Mails. Denn wer sendet schon sensible Inhalte per Postkarte?

Für den sicheren und komfortablen Zugriff von außen stellt die Firewall zudem VPN-Dienste bereit. Hier verbindet sich der Anwender über einen sicheren Tunnel mit dem Unternehmensnetzwerk. Dies kann als Einwahlverbindung, beispielsweise mobil mit dem Notebook, oder als fester Site2Site-Tunnel für außen liegende Standorte oder feste Heimarbeitsplätze erfolgen.

Netzwerk

Wer kennt es nicht? Sie laden zu einem Geschäftstermin ein und empfangen nun Ihre Gäste. Um diesen den Zugriff auf das Internet zu geben, wird der WLAN-Schlüssel bereitgestellt. In vielen Unternehmen ist eine logische Netzwerktrennung noch nicht umgesetzt, und so haben Sie Ihren Gästen, die rechtlich gesehen Dritte sind, einen Zugriff auf Ihr Netzwerk gewährt.

Wieso ist ein separates Gäste-WLAN sinnvoll? Gäste, die mit Ihnen im selben WLAN sind, könnten Schadsoftware herunterladen oder ein bereits infiziertes Gerät mit Ihrem Netzwerk verbinden.

Um nun gastfreundlich und geschützt zugleich zu sein, haben Sie die Möglichkeit einer Einrichtung eines Gäste-WLAN. Dieses Gastnetzwerk kann so eingerichtet werden, dass zwar Zugriff auf das Internet gewährleistet ist, aber kein Zugriff auf das Unternehmensnetzwerk erfolgen kann. Malware, die auf irgendeine Art auf das Smartphone eines Geräts gelangte, ist nun nicht mehr in der Lage, Zugriff auf Ihre wichtigen Dateien zu erhalten.

Sie sind oft unterwegs und benutzen teilweise öffentliche WLAN-Hotspots? Dort lauern jede Menge Gefahren für den Nutzer, denn die allermeisten Netze sind nur unzureichend abgesichert. So gibt es immer wieder Vorfälle bis hin zum Daten- oder Identitätsdiebstahl. Ausspionieren oder Hacken ist für erfahrene Angreifer dann keine große Kunst mehr und mit nur wenig Aufwand verbunden.

Sie müssen jedoch nicht auf das öffentliche Netzwerk verzichten. Mittels Aufbau eines sicheren VPN-Tunnels laufen Ihre Daten sicher durch das WLAN. Komplett anonym ist der Nutzer allerdings dennoch nicht, denn der VPN verschlüsselt zwar den Traffic und ändert auch Ihre öffentliche IP-Adresse, aber über andere Techniken können Sie immer noch als Nutzer zurückverfolgt werden, nur eben ohne Zugriff auf die übermittelten Daten.

Weitere Risiken

Zusätzliche Risiken können aber nicht nur von außen ins Unternehmen gelangen. Oft reicht schon der Fehler eines Mitarbeiters, um Daten potenziell zu gefährden. Dies geschieht natürlich nicht mit Absicht. Folgende Fragestellungen sollen hierbei eine Hilfe darstellen, um sich zusätzlicher Risiken bewusst zu werden:

Wie sieht es konkret mit dem Rechte- und Rollenkonzept im Unternehmen aus? Hier sollten klare Rollen definiert werden, denen Berechtigungen erteilt oder entzogen wer-

den können. Über Zugriffsrechte wird dann geregelt, wer im Rahmen der jeweiligen Funktion innerhalb des Unternehmens Zugriff auf sensible Anwendungen erhält.

Werden solche Rechte- und Rollenkonzepte nicht umgesetzt, kann dies zu einer Verletzung der Vertraulichkeit und Integrität von Daten gemäß Art. 32 DSGVO (= technische und organisatorische Maßnahmen) führen.

Wann ein Ausfallrisiko grundsätzlich steigt, hängt von verschiedenen Faktoren ab. Ein nicht außer Acht zu lassendes Risiko ist das Alter der Geräte. Mit zunehmender Lebensdauer steigt in jedem Fall die Ausfallwahrscheinlichkeit; hinzu kommen fehlende Updates für Systeme, die sich im End-of-Life-Zyklus befinden. Nicht nur alte Software, sondern auch nicht mehr verfügbare Ersatzteile sorgen für ein erhöhtes Risiko.

Für Computer/Notebooks und Wechseldatenträger eignet sich das Überschreiben mittels Wipe-Funktion (Einsen und Nullen). Sind diese nicht mehr ansprechbar (defekt), dann empfiehlt sich eine Vernichtung mittels Schredder über einen Dienstleister (Auftragsverarbeitungsvertrag erforderlich); für Smartphones gibt es keine Patentlösung außer Schredder.

Gibt es bei Ihnen definierte Zuständigkeiten für die Funktionalität und Instandhaltung der IT-Systeme? Übernimmt diese Funktion ein Administrator des Unternehmens, oder wird hier die Hilfe eines externen Dienstleisters in Anspruch genommen? Hier sollten ausreichend Ressourcen und maßgeschneiderte Leistungspakete vorhanden sein. Wichtig ist vor allem auch die proaktive Überwachung und Betreuung und nicht nur als Zuruf-Service im Störungsfall.

Dienste

Der Trend geht heutzutage für immer mehr Anwendungen in die Cloud. Für die Nutzung dieser Onlinedienste ist die Verfügbarkeit Ihres Internetzugangs eine der wichtigsten Grundlagen für das tägliche Arbeiten.

Egal, ob es sich hierbei um CRM-Anwendungen, Office-Anwendungen oder Bewertungstools handelt: Wenn das Internet versagt, versagen auch alle diese Dienste. Wichtig ist also, hier die richtigen Maßnahmen ganz bewusst im Vorfeld getroffen zu haben, sodass jederzeit auf eine redundante Notfallanbindung zurückgegriffen werden kann.

Größe und Menge an Daten nehmen täglich zu, doch wie übermitteln Sie große Datenmengen? Hier haben sich Austauschdienste und Plattformen etabliert, doch wo liegen die Daten? Wer hat Zugriff darauf? Stellt der Dienstleister die erforderlichen Verträge zur Verfügung, und sind Sie damit auch in Sachen DSGVO konform?

Eine häufige Alternative stellt hier die Open-Source-Lösung NextCloud dar. Diese kann bei unterschiedlichen Hostern gebucht werden.

Fazit

Die Themen sind insgesamt sehr vielschichtig. Geeignete Lösungen sind häufig für überschaubare Budgets zu haben. Schwieriger ist es dagegen, den Überblick zu behalten, da auch die Anforderungen an das Know-how ständig wachsen.

Eine passende Beratung und Betreuung eines IT-Spezialisten ist daher im Zweifelsfall empfehlenswert.

Eric Drissler
Alexander Schäfer,
ED Computer & Design GmbH & Co. KG