Cyberkriminalität

Im Sicherheitsdreieck Technik, Prozesse, Mensch

Gestohlene Kontakte, geknackte Passwörter und lahmgelegte Server gehören inzwischen zum digitalen Alltag. Betroffen sind sowohl große Konzerne als auch mittelständische Firmen – und Unternehmen der Wohnungswirtschaft bilden keine Ausnahme. Abhilfe gegen Cyberattacken und Datenklau versprechen eine individuelle Risikoanalyse und ein darauf abgestimmtes Sicherheitskonzept. Wichtig ist zudem die Sensibilisierung der eigenen Mitarbeiter.

Susanne Vieker
Prokuristin und
Mitglied der Geschäftsleitung
Haufe-Lexware Real Estate AG
Bielefeld

Wer an Sicherheitsprobleme im IT-System denkt, geht meist von technischen Lücken aus. Dabei haben Studien inzwischen ergeben, dass die ganz entscheidenden Faktoren das Sicherheitsbewusstsein und das Verhalten der Angestellten sind. Die meisten Cyberangriffe werden mittlerweile nicht durch klassische Hacker, sondern durch die eigenen Mitarbeiter verursacht – i.d.R. gar nicht vorsätzlich, sondern aus reiner Unwissenheit heraus. Die beste Technik nutzt nichts, wenn Angestellte fahrlässig handeln und z.B. vertrauliche Daten auf privaten Datenträgern mit auf Reisen nehmen.

Daten erheben, Daten schützen

Schützenswerte und sensible Daten gibt es in der Wohnungswirtschaft zuhauf. Egal, ob in großen Unternehmen oder im kleinen Betrieb: Personenbezogene Informationen – von Mietern oder Wohnungsinteressenten, von Handwerkern oder Zulieferern – werden überall erhoben und digital verarbeitet. Geraten die Daten in die falschen Hände, kann dies weitreichende Folgen für das betroffene Unternehmen haben. Neben den Schäden im eigenen System kann ein Angriff aufs IT-System auch bei Wohnungsunternehmen zu Haftpflichtschäden führen oder Datenschutzverfahren nach sich ziehen – ganz zu schweigen vom enormen Reputationsschaden und Vertrauensverlust. Unternehmen der Wohnungswirtschaft brauchen deshalb eine umfassende Sicherheitsstrategie.

CHECKLISTE ZUR BESTANDSAUFNAHME DES IT-SCHUTZBEDARFS

- Welche geschäftsrelevanten Informationen liegen digital vor?
- Wie hoch ist die Gefahr eines Schadeneintritts? Wie schnell kann dann reagiert werden?
- Welche Vorkehrungen zum Schutz von IT wurden bereits getroffen? Wie effektiv sind diese Maßnahmen in der Praxis?
- Ist das IT-Sicherheitsniveau ausreichend? Welche Sicherheitsmaßnahmen müssen noch ergriffen werden?
- Wer hat Zugriff auf geschäftskritische und personenbezogene Informationen? Wer sollte Zugriff haben, wer nicht?
- Wie kann unerwünschter interner und externer Zugriff auf diese Informationen verhindert werden?
- Wie hoch ist das Sicherheitsniveau der Lieferanten und Geschäftspartner?
- Wird der Faktor Mensch berücksichtigt?
- Wie müssen Sicherheitsmaßnahmen umgesetzt und aufrechterhalten werden? Wer ist dafür verantwortlich?

Denn tatsächlich ist das Risiko real: Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) hat in einer Studie ermittelt, dass zwei von drei Firmen (67%) in Deutschland innerhalb eines Jahres von IT-Angriffen oder anderen Sicherheitsvorfällen betroffen waren. 41% aller Firmen verzeichneten in den letzten zwölf Monaten Phishing-Attacken. Unternehmen der Wohnungswirtschaft müssen angesichts dieser Informationen aber nicht in Panik geraten: Nicht jeder Betrieb benötigt das Komplettangebot der Sicherheitsbranche. Deshalb sollten Wohnungsunternehmen zunächst einmal eine Bestandsaufnahme machen und ihren Schutzbedarf klassifizieren. Dabei hilft es, sich gemäß einem Leitfaden des Bundesamts für Sicherheit in der Informationstechnik (BSI) zum IT-Grundschutz einige grundsätzliche Fragen zu stellen (siehe Checkliste oben).

Auf diese Weise lassen sich Sicherheitslücken im eigenen Unternehmen feststellen. Das Ergebnis der Analyse ist dann der Ausgangspunkt, um die Maßnahmen zum Schutz des Unternehmens zu bewerten und zu priorisieren. Auf dieser Basis lässt sich ein für das jeweilige Unternehmen geeignetes IT-Sicherheitskonzept entwickeln. Dabei ist es wichtig, einen konkreten Plan zu entwerfen, der von der Geschäftsleitung abgesegnet wird. Darin sollten geeignete Maßnahmen zur Beseitigung von Sicherheitslücken geregelt sein. Ferner müssen natürlich die gesetzlichen Vorschriften und die dafür notwendigen technischen Erfordernisse beachtet werden.

Technik, Prozesse, Mensch

Nötig ist ein umfassendes Konzept, das die unterschiedlichen Angriffsszenarien berücksichtigt. Eine effiziente IT-Sicherheitsstrategie muss dabei

die drei Aspekte Technik, Prozesse und Mensch gleichermaßen berücksichtigen.

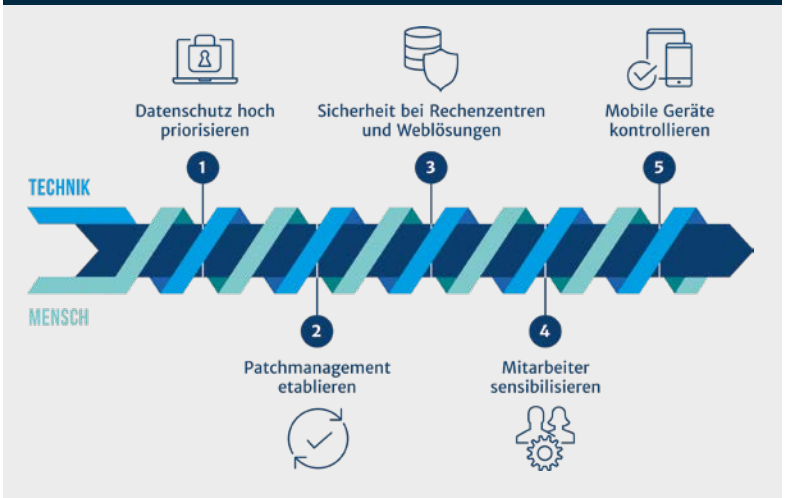
Technik

Im Bereich Technik müssen die Unternehmen vor allem für eine stabile, ausfallsichere Infrastruktur sorgen. Das erfordert Investitionen in Hardware, Software und Services. Es erfordert aber auch Entscheidungen darüber, ob die Systemlandschaft im eigenen Unternehmen oder in einem externen Rechenzentrum etwa als Cloud-Dienst betrieben werden soll. Immer noch glauben viele Firmen, die IT im eigenen Haus sei die wirtschaftlichste und sicherste Lösung. Doch das ist längst nicht mehr der Fall: Moderne Rechenzentren bieten einen Sicherheitsstandard, der im eigenen Haus nicht oder nur mit sehr großem Aufwand realisiert werden kann. Sinnvoll kann es jedoch sein, auf webbasierte Lösungen zu setzen. Webbasierte ERP-Systeme entwickeln sich beispielsweise gerade zum Standard. Es empfiehlt sich zudem, darüber nachzudenken, ob nicht weitere Elemente der IT-Landschaft webbasiert betrieben werden könnten. Bevor ein Outsourcing-Vertrag unterschrieben wird, sollte ein Unternehmen sich jedoch vor Ort von der Sicherheitsarchitektur des Anbieters überzeugen.

Prozesse

Beim zweiten Aspekt des sog. Sicherheitsdreiecks, den Prozessen, geht es darum, alle Unternehmensabläufe daraufhin zu überprüfen, ob sie den verschiedenen Bedrohungen - vom Stromausfall über Hackerangriffe bis hin zur Datensicherheit - gewachsen sind. Das beginnt bei Zutrittskontrollen im Unternehmen und erstreckt sich vom Übermitteln und Lagern von Dokumenten bis zur schnellen Anpassbarkeit der Prozesse an neue Gegebenheiten.

IN FÜNF SCHRITTEN ZU MEHR IT-SICHERHEIT



Quelle: Haufe

Mensch

Natürlich spielt auch der Faktor Mensch eine Rolle im Sicherheitsdreieck: Um die Angestellten zu sensibilisieren, muss das Unternehmen sie aus- und fortbilden und über alle sicherheitsrelevanten Fragen aufklären. Und zwar nicht nur einmal: Allein die sprunghafte Entwicklung von Technologien zwingt zum ständigen Nachjustieren. Denn nicht nur die technischen Systeme entwickeln sich weiter, sondern auch Angriffe und Bedrohungen wechseln und es gibt immer neue rechtliche Vorgaben.

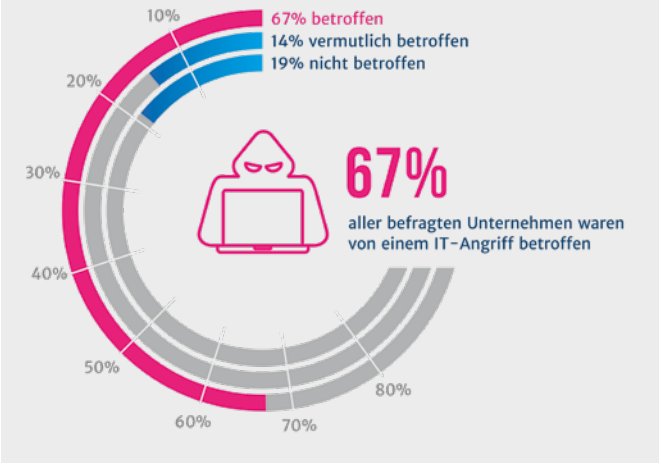
Verstärkt werden die Probleme durch mobile Geräte. Viele Wohnungsunternehmen nutzen inzwischen Tablets und Smartphones. Doch schnell bleiben die kleinen Helfer mal bei einer Wohnungsabnahme liegen oder sie fallen aus der Tasche des Mitarbeiters - der Datenklau ist ohne modernes Sicherheitskonzept dann nur noch einen Wisch entfernt. Kritisch kann es zudem werden, wenn Mitarbeiter ihr privates Gerät für dienstliche Zwecke nutzen und sensible und vertrauliche Unternehmensdaten unverschlüsselt auf ihrem Handy bearbeiten.

IT-Sicherheit ist Chefsache

Für Wohnungsunternehmen ist IT-Sicherheit eine Daueraufgabe, die auch direkt im Verantwortungsbereich der Geschäftsführung angesiedelt sein sollte. Nötig ist neben einem oder mehreren IT-Sicherheitsexperten zudem ein speziell hierfür bereitgestelltes und ausreichendes Budget, das die notwendige Konstanz und Dauerhaftigkeit finanziell absichert.

Noch ein Blick in die Zukunft: Durch weitere technische Entwicklungen - etwa das Internet of Things - entstehen neue potenzielle Sicherheitslecks. Werden im eigenen Netzwerk IoT-Geräte eingesetzt, besteht die Gefahr, dass diese angegriffen werden und Hacker Daten entwenden. Unternehmen sollten deshalb darauf achten, dass die Geräte modernen Sicherheitsstandards entsprechen.

IT-ANGRIFFE AUF UNTERNEHMEN



Quelle: Bitkom

UMGANG MIT IT-SICHERHEIT IN UNTERNEHMEN