

Führung / Kommunikation

Starker IT-Schutz für starke Unternehmen – Was zu beachten ist, erklärt Susanne Vieker, Mitglied der Geschäftsleitung der Haufe-Lexware Real Estate AG

Die Corona-Pandemie hat einen Wandel beschleunigt, bei dem sich die Wohnungswirtschaft zuvor nur sehr zögernd beteiligt hat. Spätestens seit den wiederkehrenden Kontaktbeschränkungen haben immer mehr Wohnungsunternehmen damit begonnen, mobile Arbeitsplätze einzurichten und die Kommunikation mit Mietern ins Digitale zu verlagern. Digitale Risiken wurden auf Kosten schneller Umsetzungen meist wenig beachtet. Dabei gehören Datensicherheit und Datenschutz zu den häufigsten Gründen, warum sich Wohnungsunternehmen und Mitarbeiter trotz anhaltendem Druck noch schwer tun mit der Digitalisierung. Wie sieht der Weg zu professioneller, zeitgemäßer IT-Infrastruktur aus? Der dritte von insgesamt vier Gastbeiträgen von Haufe greift die wichtigsten Risiken auf und zeigt Lösungswege für Wohnungsunternehmen und Hausverwaltungen.

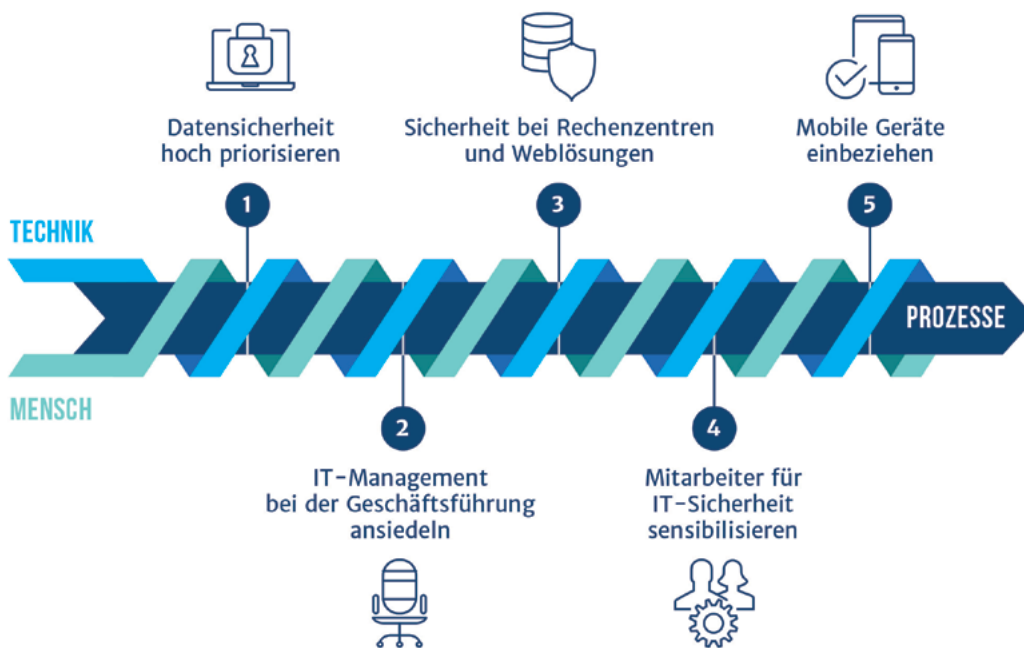


Wer mobil arbeitet, greift oft über Smartphone oder Tablet auf webbasierte Software zu. Daher müssen auch mobile Endgeräte in das Sicherheitsmanagement einbezogen werden. (Grafik: Indy_Looker / Getty Images)

Je mehr Arbeitsprozesse Unternehmen ins Digitale verlagern, desto stärker müssen sie sich vor virtuellen Angriffen schützen. Laut einer Bitkom-Umfrage haben 70 Prozent der Unternehmen in den vergangenen Jahren Cyber-Angriffe erlebt. Hacker haben es auf sensible Daten abgesehen, knacken Passwörter und installieren Ransomware. Mit dieser Schadsoftware verschlüsseln sie Computer, erpressen Firmen und legen im schlimmsten Fall den gesamten Betrieb still. Hinzu kommen rechtliche Anforderungen, Schulungsbedarf von Seiten der Mitarbeiter und eine wachsende Abhängigkeit von Stromversorgung und Internetverbindung. Auf den ersten Blick kann das erschrecken. Doch wer sich dem Thema systematisch nähert, rüstet sein Unternehmen Schritt für Schritt gegen Cyber-Angriffe.

Zentraler Hebel: Das Sicherheitsdreieck Mensch–Technik–Prozesse

Bei allen Schritten hin zu einem professionellen IT-Sicherheitsmanagement geht es darum, sowohl den Menschen, als auch die Technik und die Prozesse zu berücksichtigen. Sei es durch Unachtsamkeit oder Unwissenheit über die neuesten Technologieentwicklungen und rechtlichen Vorgaben, das größte IT-Risiko ist der Mensch selbst. Allein der richtige Umgang mit Passwörtern stellt für viele eine große Herausforderung dar, bestätigt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem neuesten Lagebericht für Deutschland. Dabei sind leistungsstarke Passwort-Manager auch als Open-Source-Software verfügbar. Da eine starke IT-Sicherheit zudem konstant angepasst werden muss und dafür ausreichend Budget benötigt wird, sollten Mitarbeiter regelmäßig geschult und das Sicherheitsmanagement direkt bei der Geschäftsführung angesiedelt werden.



Auf dem Weg zu mehr IT-Sicherheit müssen die Faktoren Mensch, Technik und Prozesse ineinandergreifen (Grafik: Haufe).

Daten, Daten, Daten – Professioneller Schutz vor unbefugtem Zugriff

Die eigenen Daten auf dem eigenen Server in den eigenen Räumen gelten vielen oft noch als bestes Sicherheitskonzept. Aber die wenigsten Wohnungsunternehmen sind mit einem so guten Sicherheitssystem ausgestattet, wie die Server von professionellen Software- und Cloudanbietern wie beispielsweise Microsoft. Letztere investieren täglich in ihre Systemlandschaft und bieten daher einen Sicherheitsstandard, den andere Unternehmen nur mit sehr großem Aufwand selbst realisieren können. Anbieter webbasierter Software weisen ihre Sicherheitsstandards durch entsprechende Zertifikate nach. Zu den Schutzmaßnahmen gehören dabei nicht nur die Verschlüsselung der Daten und das Absichern vor virtuellen Angriffen. Die Anbieter schützen ihre Infrastruktur auch vor Feuer, Einbruch und Diebstahl.

Wegen der umfangreichen Schutzmaßnahmen sind cloudbasierte Dienste der Königsweg in puncto Cyber-Schutz – sowohl in den täglichen Prozessen als auch bei der langfristigen Datensicherung. Für die Vorgaben der DSGVO ist es zudem wichtig, dass die Daten in einem deutschen Rechenzentrum liegen. Gängige Cloud-Software, wie die ERP-Software Haufe axera, erfüllen diese Anforderung. Darüber hinaus sind Standardlösungen in Bezug auf IT-Sicherheit wesentlich zuverlässiger zu handhaben und auf dem neuesten Sicherheitsstandard zu halten, als individuell programmierte oder angepasste Lösungen. Um bei der Auswahl geeigneter Cloud- und Softwareanbieter alle Belange zu berücksichtigen, sollte die Geschäftsführung relevante Fachabteilungen, die IT-Abteilung, Datenschutzbeauftragte und Hausjuristen einbeziehen. **Unerlässlich ist es, die Mitarbeiter ausgiebig und regelmäßig schulen und zu sensibilisieren.**



Ein nicht geschützter Laptop wird in den falschen Händen schnell zum Einfallstor für Cyber-Angriffe, sagt Susanne Vieker, Mitglied der Geschäftsleitung und Prokuristin der Haufe-Lexware Real Estate AG (Foto: Haufe).

Susanne Vieker

Nicht vergessen: Smartphones und andere mobile Endgeräte

Was bei einem zeitgemäßen IT-Sicherheitsmanagement zusätzlich berücksichtigt werden muss, sind Smartphones und Tablets. Sind Mitarbeiter während der Kontaktbeschränkungen kurzfristig ins Homeoffice gezogen, nutzen sie dafür oftmals ihre eigenen mobilen Endgeräte. Gehen die Geräte verloren oder werden gestohlen, können sie ein Loch in das ansonsten engmaschige Sicherheitsnetz des Unternehmens reißen. Ein nicht geschützter Laptop wird in den falschen Händen schnell zum Einfallstor für Cyber-Angriffe. Deshalb ist es entscheidend, dass auch mobile Endgeräte eine Firewall, Antiviren-Software, Passwortschutz inklusive Passwortmanager sowie regelmäßige Sicherheits-Updates erhalten. Wer noch einen Schritt weitergeht, installiert zusätzlich Sperrsoftware, welche sensible Daten bei unbefugtem Zugriff automatisch löscht. Alternativ kann der Austausch von Daten ausschließlich über webbasierte Anwendungen stattfinden. In diesem Fall werden keine Daten auf mobilen Endgeräten gespeichert.

Einen Anhaltspunkt, wo im Wohnungsunternehmen der größte Schutzbedarf liegt und welche Bereiche bei der Professionalisierung des IT-Managements priorisiert werden sollten, gibt die Checkliste von Haufe:

- + **Welche geschäftsrelevanten Informationen** liegen digital vor und müssen geschützt werden?
- + **Gibt es bereits Maßnahmen** zum Schutz von IT, wurden sie von einem professionellen Dienstleister getestet und sind die Maßnahmen ausreichend?
- + **Ist festgelegt**, wer Zugriff auf geschäftskritische und personenbezogene Daten hat und gibt es jemanden, der einen Überblick über diesen Zugriff hat?
- + **Erfüllen Lieferanten**, Geschäftspartner sowie Cloud- und Softwareanbieter ein ausreichendes Sicherheitsniveau und schützen personenbezogene Daten?
- + **Werden die Mitarbeiter** regelmäßig geschult (z.B. zum Umgang mit Passwörtern und Phishing-Mails)?
- + **Ist der sicherheitskonforme Umgang** mit sensiblen Daten, Passwörtern und ggf. mobilen Endgeräten in die Mitarbeitervereinbarungen aufgenommen?
- + **Gibt es einen Verantwortlichen** für IT-Sicherheit, ausreichend Zeit und Budget, um stets auf dem neuesten Stand der Entwicklung zu sein?