Die Wohnungswirtschaft

DW

78. Jahrgang

06 / 2025

Es tut sich was: aktuelle Entwicklungen am ERP-Markt

Seite 56

Thema des Monats

C 3188

Mat.-Nr. 06504-2384

TDM CYBERSICHERHEIT

Der Schutz gegen die unsichtbare Gefahr

Seit Jahren steigt die Zahl der Angriffe und Schäden bei deutschen Unternehmen durch Cyberkriminalität. Statistisch gibt es alle 39 Sekunden einen Angriff – auch gegen Vermieter. Wie können sich Wohnungsunternehmen schützen? Berichte aus der Praxis zeigen wichtige Handlungsfelder auf.

Von Holger Hartwig

Holger Hartwig
Agentur Hartwig 3c
HAMBURG/LEER

Noch in den Anfängen bei der Entwicklung eines umfänglichen Schutzkonzeptes gegen kriminelle Hacker steckt die Wohnungsgenossenschaft Eberswalde 1893 eG (1893). Tino Fischer ist bei der Genossenschaft im Fachbereich „Field of Experts“ für das Management digitaler Tools, Prozesse und Daten verantwortlich. Er sagt: „Natürlich prüfen wir gemeinsam mit unseren Partnerfirmen regelmäßig, wie wir mit Blick auf die Datensicherheit bei unseren technischen Anlagen und in der gesamten IT aufgestellt sind. Aber wir wissen, dass wir noch strategischer und kontinuierlicher an dem Thema arbeiten müssen, um uns in Zeiten steigender Datenkriminalität zu schützen.“

Umgang am Tag X ist entscheidend

Es reiche beispielsweise nicht mehr aus, dass – wie bei der 1893 seit Jahren gewährleistet – alle Daten auf externen Servern gesichert sind. „Unser Kerngeschäft ist die Wohnungswirtschaft. Das Kerngeschäft der Cyberkriminellen ist der erfolgreiche Angriff auf Unternehmen“, macht Fischer die Herausforderung deutlich. Es gehe darum, die Möglichkeiten des Fremdzugriffs auf die IT-Infrastruktur inklusive aller technische Anlagen, die die 1893 in ihren Häusern einsetzt, systematisch zu verringern. Für Fischer sind – neben der guten Zusammenarbeit mit allen Herstellern IT-gestützter Anlagen – die Mitarbeitenden die Hauptherausforderung. „Allen 52 Mitarbeitenden muss im täglichen Umgang mit der Technik bewusst sein, dass es nicht mehr um die Frage geht, ob wir durch Cyberkriminelle angegriffen werden, sondern wie wir am Tag X mit einem Angriff professionell umgehen.“

Gemeinsam mit den Partnerfirmen und Spezialisten würden seit Jahresbeginn 2025 intensiv – auch mit Phishing-Angriffen – alle digitalen Prozesse auf Schwachstellen durchleuchtet. Fischer: „Wie in jedem anderen Unternehmen ist auch bei uns der User und sein Umgang mit den digitalen Werkzeugen eine der größten Herausforderungen.“ Deshalb habe man in einem zweiten Schritt Ende April zu einem Workshop eingeladen, um das Bewusstsein der Mitarbeitenden zu stärken. Es müsse gelingen, jedem Mitarbeitenden zu verdeutlichen, dass die Frage der digitalen Sicherheit „nicht irgendwo in einem dunklen Keller beantwortet wird, sondern vor allem durch die permanente Achtsamkeit eines jeden Systemnutzers“. Fischer: „Entscheidend ist dann, dass es einen funktionierenden Austausch im Unternehmen gibt. Bei uns kann über ein Ticketing-System jeder Mitarbeitende schnell und unkompliziert das IT-Team über Auffälligkeiten informieren.“

IT-Sicherheit im Unternehmen ist nicht nur Sache der IT

„Die IT-Sicherheit macht bei uns die IT“ – dieses Denken der Mitarbeitenden war bei der Kommunalen Wohnungsgesellschaft mbH Erfurt (Kowo) vor drei

Foto: Javier Zayas Photography/gettyimages.de

Digitale Daten brauchen Schutz: Wohnungsunternehmen sichern sich zunehmend gegen Cyberangriffe – technisch, organisatorisch und durch geschulte Mitarbeitende

Jahren bei der Prüfung sämtlicher Prozesse sowie aller technischen Anlagen auf IT-Sicherheitsrisiken eine der zentralen Erkenntnisse. Patrick Ziegler, der bei dem Erfurter Unternehmen Ansprechpartner für die IT-Sicherheit ist, erinnert sich: „Wir mussten feststellen, dass der sichere Umgang mit Technik und Daten im Arbeitsalltag häufig als unscheinbare Aufgabe wahrgenommen wird und daher bislang bei vielen Mitarbeitenden nicht im Mittelpunkt stand. Umso wichtiger ist es, das Bewusstsein für dieses Thema gezielt zu schärfen und seine Bedeutung stärker in den Fokus zu rücken." Bei dem abteilungsübergreifenden Projekt lag – neben der Bestandaufnahme aller relevanten Strukturen – der Fokus auf der Frage: Wie leben die Kowo-Mitarbeitenden das Thema IT-Sicherheit? Dabei ging es um den Umgang mit Passwörtern, dem Sperren von PCs sowie um die Herangehensweise bei eingehenden E-Mails. So habe man sich als Erstes an der Phishing-Mail-Simulation des Verbands Thüringer Wohnungs- und Immobilienwirtschaft e.V. (vtw) beteiligt. Ziegler: „Es hat sich gezeigt, dass das Verhalten der Mitarbeitenden maßgeblich zur Risikolandschaft im Unternehmen beiträgt."

IT-Sicherheit mit Strategie durch Schulungen und Tests

Erste Gespräche mit Mitarbeitenden zu diesen Themen hätten nicht den gewünschten Erfolg gebracht und „uns wurde klar, dass wir eine umfassende Strategie benötigen." Unter Einbeziehung des ›

Die verschiedenen Arten von Cyberattaken

Als Cyberattacke wird ein unzulässiger, vorsätzlicher Zugriff auf das IT-System bezeichnet, der mit dem Ziel erfolgt, das angegriffene Unternehmen materiell, technisch oder finanziell zu schädigen. Dabei geht es um das Offenlegen, Deaktivieren, Zerstören oder Verändern von Daten.

Ransomeware-Attacke
Die Zielsetzung dieses Angriffs ist das „Aussperren" eines Unternehmens aus den eigenen Systemen oder das Verschlüsseln von Daten. Das Unternehmen wird erpresst, erst nach einer Lösegeldzahlung wird der Zugriff auf die Daten wieder freigegeben.

DDoS Rekord-Angriff
Bei diesem Angriff handelt es sich um das gezielte Lahmlegen von Systemen durch bewusst erzeugte Überlastung dieser Systeme. Es werden fremde Netzwerke „gekapert", um die Funktionsweise der Dienste zum Zusammenbruch zu bringen.

Datendiebstahl
Diese Attacke ist weitgehend bekannt. Ziel ist es, mit den unterschiedlichsten Methoden auf sensible Daten (Bank- und Kreditkarteninformationen, Kundendaten) zuzugreifen und diese weiter zu verkaufen. Für das betroffene Unternehmen ist ein derartiger Diebstahl mit viel Aufwand und einem Vertrauensverlust bei den Kunden verbunden

Netzwerkangriff
Bei diesem kriminellen Akt geht es darum, in ein Netzwerk einzudringen und Daten abzugreifen oder Funktionsweisen eines Netzwerkes, zum Beispiel auch Heizungsanlagen oder Zugangssystemen zu Häusern, zu beeinträchtigen.

INTERVIEW MIT UDO WALTHER

„Jeder muss mit einem Cyberangriff rechnen."

Die bestmögliche Absicherung im Falle eines kriminellen Hackerangriffs – das ist das Ziel einer Cyberversicherung. Der Versicherungsfachmann Udo Walther hat sich auf die Beratung von Wohnungsunternehmen spezialisiert. Der Regionalleiter Versicherungen bei der Dr. Klein Wowi Finanz AG zeigt auf, worauf es ankommt.

Herr Walther, nennen Sie die drei wichtigsten Gründe, warum eine Cyberversicherung für ein Wohnungsunternehmen eine Selbstverständlichkeit sein sollte.

Es ist unbestritten, dass jedes Unternehmen, das ein Datennetzwerk betreibt, mit dem Risiko leben muss, Ziel eines Hackerangriffs zu werden. Aktuelle Statistiken sagen aus, dass mehr als 80 % aller deutschen Unternehmen über alle Branchen hinweg bereits Opfer oder Ziel eines Cyberangriffs waren. Kurzum: Jeder muss damit rechnen, dass es ihn früher oder später – salopp formuliert – „erwischt". Die Versicherung ist dann aus mehreren Gründen sehr hilfreich: erstens, um den Schaden durch professionelle Unterstützung im Umgang mit den Angreifern zu minimieren, zum Zweiten, um die Arbeitsfähigkeit so schnell wie möglich wiederherzustellen, zum Dritten, um Kosten für die Betriebsunterbrechung im eigenen Hause refinanziert zu bekommen, und zum Vierten, um sich auch gegen Forderungen von dritter Seite, beispielsweise durch Verstöße gegen die Datenschutzgrundverordnung, abzusichern. Denn: Jeder erfolgreiche Angriff, der sich auf personenbezogene Daten ausgewirkt hat, ist bei der zuständigen Aufsichtsbehörde zu melden.

Gibt es bereits Erfahrungen mit Angriffen auf Wohnungsunternehmen?

Ja, wir hatten bei unseren Kunden, die heute zu 90 % eine Versicherung haben, bereits mehrere Fälle. Beispielsweise wurde der Kommunikationsserver inklusive der Telefonanlage lahmgelegt, so dass Kontakt zu Kunden und Geschäftspartnern über mehrere Wochen nicht möglich war. Bei einem anderen Fall wurde die Buchhaltung durch einen Angriff angewiesen, offene Posten an einen Bauunternehmer zu überweisen, was leider fälschlicherweise auch gemacht wurde. Das überwiesene Geld – einige tausend Euro – war weg. Grundsätzlich muss man feststellen: Die Angriffe unterscheiden sich nicht von den Attacken auf andere Branchen. Den Kriminellen ist es vollkommen egal, wo sie erfolgreich sind. Die Schäden reichen bei den Angriffen bis hin zu Millionenbeträgen, im Durchschnitt sind es laut Gesamtverband der deutschen Versicherungswirtschaft (GDV) aktuell 45.000 €.

Welche Daten sind für Hacker bei einem Vermieter am interessantesten und sollten daher im Fokus des Schutzes stehen?

Bekannt sind aktuell vier Arten von Angriffen: 2023 ist bei einem Unternehmen in Berlin die gesamte Infrastruktur lahmgelegt worden. Die Mieterdaten wurden verschlüsselt, insgesamt ging der Schaden in die Millionen. Zweites Angriffsziel sind Manipulationen an Überwachungssystemen, beispielsweise an der Eingangstürsteuerung von Häusern. Hier musste das betroffene Unternehmen mehrere Monate daran arbeiten, bis alles wieder funktionsfähig war, auch das kostete einen siebenstelligen Betrag. Drittes Beispiel ist ein Eingriff in die Datencloud: Hier waren etwa Daten von 1.000 Mieterinnen und Mietern öffentlich zugänglich, was zu Strafen wegen Verstößen gegen den Datenschutz führte und der Reputation des Unternehmens massiv geschadet hat und zu zusätzlicher Mieterfluktuation geführt hat.

Das letzte Beispiel kommt aus dem Bereich des Internet-of-Things (IoT): Es war ein Angriff auf die Heizungsanlagen und die Fahrstühle, die Heizungen wurden abgeschaltet und die Mieter haben darauf die Mieten gekürzt. Es gibt ausreichend Einfallstore, die – wenn ein Angriff erfolgreich ist – für die Vermieter massive Schwierigkeiten mit sich bringen können.

Worauf sollten die Wohnungsunternehmen achten, wenn Sie eine Cybersecurity-Versicherung abschließen wollen?

Ich sehe drei wesentliche Punkte: Der Anbieter sollte den Baustein Forensische Dienstleistungen im Portfolio haben, das heißt, IT-Spezialisten sollten sich um den Cybervorfall sofort kümmern. Die Qualität der Anbieter unterscheidet sich durchaus, deswegen sollten die Kosten für die Police nicht ausschließlich entscheidend sein. Die günstigste Police muss nicht immer die beste sein. Zum Zweiten sollte immer auch darauf geachtet werden, dass neben Eigenschäden auch Haftpflichtschäden an Dritten abgedeckt werden. Dritter Aspekt sind die Vertragsbedingungen mit dem Punkt Obliegenheiten. Dabei geht es um die Frage, wozu die Unternehmen als Versicherungsnehmer verpflichtet sind. Hier kommt es auf exakte Formulierungen an, beispielsweise, ob das Unternehmen nachweisen können muss, dass immer der aktuellste Stand der Software auf allen eingesetzten Geräten installiert war. Gute Versicherer machen vor Vertragsabschluss zudem eine gute Analyse und checken durch Tests ab, ob und wo der Versicherungsnehmer Einfallstore haben könnte.

Wie hoch sind die Kosten für eine gute Cyberversicherung?

Meine Erfahrung ist, dass die meisten Geschäftsführer und Vorstände überrascht sind, wie niedrig die Kosten sind. Es kommt natürlich darauf an, welche Schutzbausteine gewählt werden und wie groß das Unternehmen ist. Einen guten Versicherungsschutz kann es bereits bei jährlichen Kosten ab 1.500 € geben.

Vielen Dank für das Gespräch.

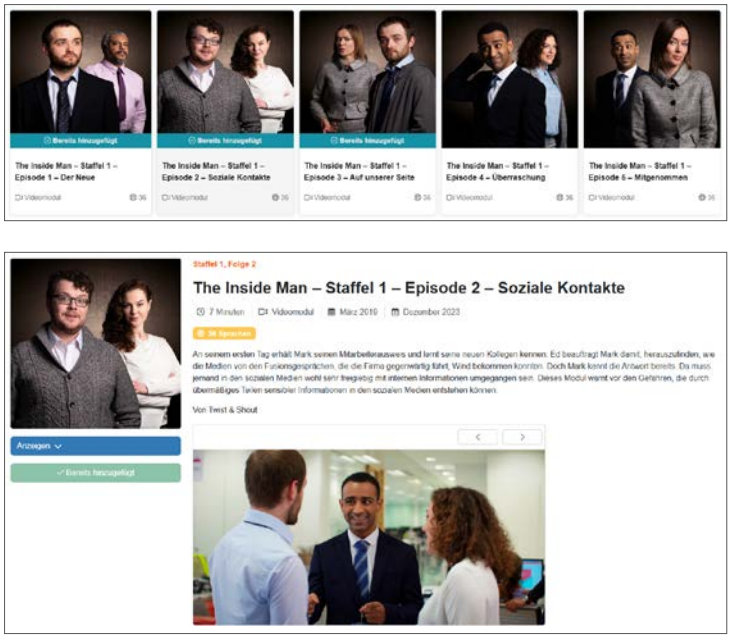
Das Interview führte Holger Hartwig

Bilder: Dr Klein; Kowo

Betriebsrates habe man eine Informationskampagne aufgesetzt und sich mit den Firmen Cancom und Knowbe4 unter anderem für Penetrationstests beziehungsweise professionelle Schulungen zwei erfahrene Partner gesucht. Mit der Firma Cancom wurde eine erste umfassende Analyse des Status Quo vorgenommen. „Eine sehr erdende Erfahrung war das Thema Passwortstruktur. Die Experten haben es in einem Test innerhalb von sechs Stunden geschafft, aus verschiedenen Datenbanken Infos zu generieren. Bei den Rechnern, bei denen der Zugriff gelang, wurde der Mailversand übernommen. Das war ein Aha-Effekt für das gesamte Haus." Viele hielten sich bei der Passwortwahl zwar formal an die Vorgaben – etwa Großbuchstaben, Zahl und Sonderzeichen –, setzten diese aber in vorhersehbarer Reihenfolge um. Ziegler: „Wir haben ein internes Schulungskonzept aufgestellt, welches unter anderem aus Präsenz-Schulungen und wiederabspielbaren Lernvideos besteht. Beispielsweise schulen wir, was ein sicheres Passwort benötigt und wie man es erstellt." Mit der Herangehensweise sei es zusätzlich gelungen, das Verständnis für die Gefahren eines ungesperrten Rechners stark zu stärken. Zweites Projekt war ein strukturierter Phishingtest auf Basis der Knowbe4-Plattform. Ziegler: „Wir haben den Test am Ende alle zwei Wochen vorgenommen. Die Mitarbeitenden haben immer besser verstanden, dass sie selbst ein ganz wesentlicher Teil der IT-Sicherheit sind."

Niedrigschwelliger Ansatz mit Schulungsvideos im Netflix-Stil

Worauf es mit Blick auf mehr Sicherheit ankommt? Auf die Kontinuität. Ziegler: „Sicherheitsthemen erfordern eine kontinuierliche Erinnerung – eine einmalige Maßnahme genügt nicht, um langfristiges Bewusstsein und sicheres Handeln zu verankern."



Bei der Kowo in Erfurt wird die Cyberschulung per Videos im Netflix-Stil durchgeführt

Der Kowo sei ein niederschwelliger Ansatz wichtig. „Die Mitarbeitenden erhalten nun beispielsweise einmal im Quartal ein Schulungsvideo im Netflix-Stil mit einer Länge von bis zu sieben Minuten." Als zweiten Erfolgsfaktor sieht der IT-Experte, dass die Mitarbeitenden auf Meldungen an die IT immer ein ›

Feedback bekommen. „Wir haben einen Meldebutton für Phishing-Verdachtsnachrichten in Outlook integriert. Über diesen Button haben wir viel mehr an Informationen bekommen. Im Haus ist sogar eine kleine Challenge entstanden, wer die meisten Fake-Mails identifiziert."

Wie es weitergeht? Ziegler: „Wir werden gezielt weitere Penetrationstests durchführen, auch mit Elementen des Social-Engineering. In Zukunft kommt dann vielleicht auch Mal ein Techniker, der sich als Telekom-Mitarbeiter ausgibt, so dass wir beobachten können, ob und wie weit er im Unternehmen an technischen Anlagen frei agieren kann."

Dank Versicherung „glimpflich davongekommen"

Während sich die 1893 und die KoWo vor Angriffen schützen, weiß die Märkische Baugenossenschaft eG mit Sitz in Berlin-Charlottenburg bereits, wovon die Rede ist, wenn es um das Unwesen von kriminellen Datenjägern geht. Neben dem technischen Aspekt geht es dann auch um die Frage der Wahl der richtigen Versicherung – am besten, bevor der erste Cyber-Angriff erfolgt. In dieser Hinsicht hatte die Märkische Baugenossenschaft eG im Jahr 2021 Glück, dass bei einem Angriff auf das IT-System – es gab eine Sicherheitslücke bei Microsoft, die Hacker nutzten, bevor die offizielle Warnung an die Kunden erfolgt war – eine Versicherung bereits abgeschlossen war. Thomas Erdt, Vorstand der Baugenossenschaft, erinnert sich: „Ohne die Versicherung, die uns sofort unterstützt hat, wären wir damals nicht so glimpflich davongekommen." Nach den Erfahrungen vor vier Jahren habe man das Thema IT-Sicherheit auf allen technischen Ebenen neu betrachtet und dabei alle Mitarbeitenden gezielt eingebunden.

Restrisiko eines erfolgreichen Angriffs besteht immer

Aus Sicht von Erdt ist es wichtig, dass sich die Branche bewusst werde, dass es viele Bereiche gibt, bei denen Daten abgegriffen oder Technik fremd gesteuert oder gar lahmgelegt werden könnte. „Das reicht von Immobiliendaten, Informationen zu den Mietern und Abrechnungsdaten bis hin zu Zugriffen auf die Steuerung der Haustechnik oder die digitalen Schließsysteme." Für Erdt steht fest, dass bei allen Vorsichtsmaßnahmen immer ein Restrisiko eines erfolgreichen Angriffs bleibt, da die Einfallstore für Hacker so zahlreich sind. „Eine Cyberversicherung ist aus meiner Sicht ein Muss. Wenn der Fall der Fälle eintritt, dann ist es unverzichtbar, innerhalb kürzester Zeit Unterstützung durch den Versicherer zu erhalten." Ohne die Versicherung und deren Experten hätten sie nicht gut ausgesehen. „Man kann mit einem solchen Schutz deutlich besser schlafen", ist sich Erdt sicher – und hofft, dass seine Genossenschaft so schnell die Versicherung nicht wieder in Anspruch nehmen muss.

Bausteine der Cybersversicherung

Prävention
- Risikoanalyse
- Erstellung eines Cyber-Krisenplans
- Sensibilisierung für Mitarbeiter
- Online-Trainings

Haftpflichtansprüche
- Prüfung fremder Ansprüche gegen das Unternehmen
- Abwehr oder Erfüllung

Eigenschäden
- in Folge Erpressung, Betrug und Diebstahl
- Bedienfehler
- Hard- und Software

Betriebsunterbrechung
- Ertragsausfall
- Fortlaufende Kosten

Quelle: Dr. Klein

Vier Handlungsfelder nach einem Cyberangriff

Auch Robert Kutscher, Prokurist und Leiter Personal/Organisation/IT bei der Wohnungsgesellschaft Schwerin mbH (WGS), weiß, wovon er spricht, wenn er über Datensicherheit redet. Ein Angriff auf die WGS im Jahr 2021 sorgte für einen Gesamtschaden mit sechstelliger Euro-Summe. Kutscher: „Wir haben daraus viel gelernt und sind überzeugt: Wenn wir noch einmal angegriffen werden sollten, dann bleiben wir handlungsfähig." Er definiert für die Cybersicherheit vier zentrale Aspekte: „Als erstes sollte jedes Unternehmen für sich definieren, was die überlebenswichtigen Prozesse, wie zum Beispiel das Lastschriftverfahren, sind, und klären, welche Technologie dahintersteckt und wie eine Absicherung durch Notfall- und Sicherheitspläne erfolgen kann." Zweiter Aspekt ist die wirtschaftliche Absicherung und die Frage der Unterstützung im Angriffsfall durch die Cyberversicherung. „Wichtig ist, darauf zu achten, dass auch die Betriebsunterbrechung mitversichert ist. Zudem sollte auch geprüft werden, ob die IT-Dienstleister ebenfalls versichert sind." Als drittes rät der WGS-Prokurist, dass die Mitarbeitenden immer wieder für diese Thematik sensibilisiert werden müssen, „auch wenn das nervig und herausfordernd ist". Zu guter Letzt ist Kutschers Empfehlung, auch eine durchdachte Kommunikationsstrategie in der Schublade zu haben. „Mieter und Geschäftspartner sollten umgehend informiert werden, wenn ein Cyberangriff erfolgt ist, damit sie wissen, was die Auswirkungen sind und was sie gegebenenfalls zu machen hätten." Denn eines hat Kutscher neben dem Schaden in Erinnerung behalten: Bis das Unternehmen wieder voll funktionsfähig war, hat es 2021 etwa drei Monate gedauert und der Schaden sei nicht nur in wirtschaftlicher Hinsicht erheblich gewesen. —

HAUFE

4 Wochen kostenlos testen

Rechtssicher. Zeitsparend. Effizient.

Aktuelles Fachwissen und praktische Arbeitshilfen

- Inklusive der Formulare und Verträge des GdW
- **Nachhaltigkeit: CO_2-Monitoring, Balkon- und PV-Anlagen sowie grüne Finanzierung**

Testen Sie WohnungsWirtschafts Office Professional mit rechtssicherem Know-how, topaktuellen Infos und Arbeitshilfen für Ihren Erfolg in der Wohnungswirtschaft.

haufe.de/wowi-pro