Daten und Geschäftsprozesse schützen

Die Sicherheit der Cloud ist ein strategisches Thema

Die Angst vor Cyber-Attacken ist weit verbreitet. Dabei sind nicht nur Konzerne und kritische Infrastrukturen bedroht. Jedes Unternehmen, das cloudbasierte Dienste in Anspruch nimmt, hat ein erhöhtes Risiko. Dazu gehören auch Wohnungsunternehmen und Hausverwaltungen.

Dabei haben solche Attacken unterschiedliche Folgen – von Imageschäden über Umsatzeinbußen und den Verlust geschäftskritischer Daten bis hin zu Beeinträchtigungen der Arbeitsprozesse oder gar dem kompletten Stillstand des Unternehmens. Darum gilt es, sich mit Cloud Security zu beschäftigen und ein Verständnis der Thematik zu erwerben.

Daten bleiben ungeschützt

Sind Hacker erst einmal in die IT-Infrastruktur eingedrungen, dauert es rund 100 Tage, bis dies auffällt. Drei Monate, in denen Cyber-Kriminelle großen Schaden anrichten können. Dabei geht mancher Hacker sehr subtil vor, etwa indem er Bilder ein klein wenig manipuliert oder vermeintlich unbedeutende Informationen abgreift. Unabhängig von den Folgen eines solchen Angriffs ist es Fakt: Viele Hausverwaltungen und Wohnungsunternehmen schützen ihre Systeme, Daten und Geräte in der Cloud nicht, weil sie sich der Problematik nicht bewusst sind. Was also ist zu tun, damit die Cloud-Migration nicht zum Sicherheitsrisiko wird?

Individuell anpassbare Standard-Lösungen nutzen

Wer die Lösungen der etablierten Cloud-Anbieter nutzt, ist auf dem richtigen Weg. Sie bieten bereits im Standard viele Tools und Konfigurationsmöglichkeiten, mit denen sich ein gutes Maß an Cloud Security sicherstellen lässt. Wer sie darüber hinaus individuell anpassen oder generell Cloud-Lösungen entwickeln lässt, sollte einen spezialisierten Dienstleister beauftragen, der den Infrastructure-as-Code-Ansatz (IaC) verwendet. Dies erlaubt, sicherheitsrelevante Features direkt im Quellcode zu hinterlegen und abgesicherte Infrastruktur-Templates für weitere Zwecke zu duplizieren.
Daneben müssen Wohnungsunternehmen und Hausverwaltungen jegliche Daten und Systeme in der Cloud lückenlos inventarisieren: Welche Plattformen gibt es? Wer ist verantwortlich? Wer administriert welche Plattform? Welche Daten gelangen auf welche Plattform? Woher kommen sie? Wohin fließen sie? Wie? Und warum?

FOTO: PEOPLEIMAGES.COM / STOCK.ADOBE.COM

Die Auslagerung von Unternehmensdaten in externe Rechenzentren (Cloud-Lösungen) erfordert eine besondere Sicherheitsphilosophie im Hause des Kunden.

Cloud Security als Geschäftsprozess begreifen

Den aktuellen Status aller Cloud-Anwendung zu kennen, ist eine grundlegende Voraussetzung, um Cloud-Sicherheit als Business-Prozess verstehen zu können. Als Prozess, der mit Bedacht modelliert, mit Metriken gesteuert, mit Tools überwacht und kontinuierlich optimiert sein will. Zum Prozessmanagement gehören auch regelmäßige Audits. Während dies bei internen Firmen-Netzwerken üblicherweise im Jahresrhythmus geschieht, lassen sich externe cloudbasierte Anwendungen täglich oder gar stündlich im Hinblick auf etwaige Sicherheitslücken scannen. So sind Schwachstellen kurzfristig identifizier- und effektiv schließbar.

Alles und jeden verifizieren

Im Cloud-Umfeld wirken ältere Schutzmechanismen nicht mehr. So ist etwa eine Firewall völlig ungeeignet, wenn Daten in der Cloud liegen. Stattdessen sind alle Systeme und sämtliche Endgeräte gegen unerlaubte Zugriffe abzusichern (Zero Trust) – insbesondere, wenn Teammitglieder außerhalb des Firmen-Netzwerks im Homeoffice arbeiten. Zero Trust bedeutet: „Vertraue niemandem außerhalb und innerhalb deiner Organisation. Und verifiziere jeden."

Doch Zero Trust ist keine Lösung, die sich per Knopfdruck freischalten lässt, sondern ein Designprinzip, das individuell umzusetzen ist. Greifen zum Beispiel Mitarbeiter über Firmen-Smartphones auf ihre E-Mail-Postfächer zu, ist das unbedenklich, weil Nutzer und Geräte bekannt sind. Benutzen sie jedoch private Mobilgeräte, ist Vorsicht geboten. Idealerweise gibt es für solche Fälle einen zweiten Faktor, über den sich Mitarbeiter authentifizieren.

Schutzziele definieren

Diese Multi-Faktor-Authentifizierung ist eines von vielen Schutzzielen, die Hausverwaltungen und Wohnungsunternehmen definieren sollten: Damit Mitarbeiter cloudbasierte Lösungen benutzen dürfen, ist ein zweites Authentifizierungsmerkmal an allen Geräten und Endpunkten zu installieren. Denn die Frage ist nicht, ob Unternehmen gehackt werden, sondern wann. Mit einer zweiten Identifizierungsstufe, wie etwa einer

SMS, einer App, einem Anruf oder einem weiteren Gerät, lässt sich das Risiko deutlich verringern. Zudem empfiehlt sich bei BYOD-Szenarien (Bring Your Own Device) eine Null-Toleranz-Politik: Erfüllen private Endgeräte die Sicherheitsanforderungen nicht, dürfen sie nicht mit dem Netzwerk verbunden sein. Ebenso ist zu prüfen, ob das Patch-Management (Durchführung von Software-Updates) im Homeoffice wirkungsvoll ist.

Daten und Dateien zentral schützen

All diese Einzelmaßnahmen basieren auf zwei zentralen Frage: Was darf Daten, Dateien, Geräten, Datenbanken und Services passieren? Und wer ist berechtigt, das zu tun? Idealerweise sind diese Informationen personenbezogen und zentral hinterlegt: Wer ist eine Person? Welche authentifizierten Geräte nutzt sie? In welchem Zustand befindet sich ein Gerät (beruflich, privat, gepatcht etc.)? An welchen Orten (Zentrale, Niederlassung, Kunden etc.) hält sich die Person üblicherweise auf? In welchem Status befinden sich die Konten und Profile der Person (gerade gehackt oder sicher)? Anhand dieser und weiterer Informationen lassen sich erlaubte von unautorisierten Zugriffen recht zuverlässig unterscheiden.

Warum es mehr Verständnis für das Thema braucht

In Sachen Cloud Security ist also viel zu tun. Doch weil dies wenig mit dem Alltag von Hausverwaltungen und Wohnungsunternehmen zu tun hat, fehlt vielerorts das Verständnis dafür, wie wichtig Cloud Security für einen reibungslosen Geschäftsbetrieb ist. Dringen Cyber-Kriminelle zum Beispiel in die IT-Infrastruktur einer großen Hausverwaltung ein, kann sie womöglich keine Nebenkosten abrechnen. Eine Cyber-Attacke trifft sie also dort, wo sie am verwundbarsten ist: bei ihren Kernprozessen. Darum sollten sich Verantwortliche damit beschäftigen, welche Möglichkeiten die Cloud eröffnet – und welche Security-Maßnahmen sinnvoll sind. Cloud-Sicherheit ist komplex – keine Frage. Umso wichtiger ist es, dass der Praxisbezug im Vordergrund steht. So hängt der wirtschaftliche Erfolg eines Wohnungsunternehmens auch daran, dass es Mietverträge schließen kann. In Sachen Cloud Security muss es also unter anderem darum gehen, dass in der Cloud gespeicherte Vertragsunterlagen jederzeit zugänglich sind. Ein Verständnis für diese Thematik unter allen Beteiligten zu schaffen, ist jedoch nur der erste Schritt. Perspektivisch ist Cloud Security in der Unternehmensstrategie dauerhaft zu verankern – und natürlich praktisch umzusetzen. Dies sind Herausforderungen, die weit über die IT hinausgehen. Darum müssen für eine wirkungsvolle Cloud Security alle an einem Strang ziehen.

Autor
Andreas Nolte,
Head of Cyber Security
Arvato Systems

BSI-Lagebericht zur IT-Sicherheit 2023

Täglich 70 neue Schwachstellen in Software-Programmen

Die Bedrohung im Cyberraum ist so hoch wie nie zuvor. Zu diesem Fazit kommt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Jahresbericht zur Lage der IT-Sicherheit in Deutschland.

Bei Cyberangriffen mit Ransomware (Erpresser-Trojaner, die Computer lahmlegen) beobachtet das BSI eine Verlagerung der Attacken: Nicht mehr nur große, zahlungskräftige Unternehmen stünden im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen. Insbesondere von erfolgreichen Cyberangriffen auf Kommunalverwaltungen und kommunale Betriebe seien Bürgerinnen und Bürger oft unmittelbar betroffen.
Wie die Realwirtschaft setzten auch Cyberkriminelle zunehmend auf Arbeitsteilung, einen wachsenden Dienstleistungscharakter und eine enge Vernetzung über Länder- und Branchengrenzen hinweg. Mit dem Konzept des „Cybercrime-as-a-Service“ agierten Cyberkriminelle immer professioneller, denn die Spezialisierung auf bestimmte Dienstleistungen ermögliche es ihnen, ihre „Services“ gezielt zu entwickeln und einzusetzen. Das BSI registriert immer mehr Schwachstellen in Software. Diese Schwachstellen seien oft das Einfallstor für Cyberkriminelle auf ihrem Weg zu einer Kompromittierung von Systemen und Netzwerken. Das BSI habe mit durchschnittlich knapp 70 neuen Schwachstellen in Software-Produkten pro Tag nicht nur rund ein Viertel mehr registriert als im Berichtszeitraum davor. Mit der Anzahl stieg auch ihre potenzielle Schadwirkung: Immer mehr Lücken (etwa jede sechste) werden als kritisch eingestuft.
Mit ChatGPT, Bard und LlaMa sowie einer Vielzahl weiterer Tools ist Künstliche Intelligenz in einer breiten, auch wenig technikaffinen Öffentlichkeit angekommen. Diese Tools sind einfach zu bedienen und liefern eine hohe Qualität. Dabei können sie auch für kriminelle Zwecke missbraucht werden. So können sie dafür sorgen, dass sogenannte Deepfakes – manipulierte Bilder, Videos und Stimmen – immer authentischer werden und dadurch immer schwerer zu entlarven sind. Auch könne KI Phishing-Mails glaubwürdiger machen, im Social Web zu Desinformationskampagnen beitragen oder selbst Schadcode generieren – und das wesentlich schneller und zum Teil wesentlich besser als menschliche Cyberkriminelle. KI könne auch selbst zur Schwachstelle werden. Sie könne gehackt und missbräuchlich eingesetzt werden. Das stelle das Schwachstellenmanagement in Unternehmen und Behörden vor noch nie dagewesene Herausforderungen.
Der Branchenverband Bitkom bekräftigt, dass sich Cyberangriffe zu einer der größten Bedrohungen für unsere Wirtschaft und Gesellschaft entwickelt hätte. Längst gehe es nicht mehr um den Ausfall einzelner Computer oder auch IT-Systeme. Cyberattacken könnten die Geschäftstätigkeit eines Unternehmens vollständig lahmlegen, sie könnten notwendige Operationen in einem Krankenhaus verhindern, Kraftwerke ausschalten oder Flughäfen und Bahnstrecken zum Stillstand bringen. Jedes zweite Unternehmen in Deutschland stimme mittlerweile der Aussage zu, ein erfolgreicher Cyberangriff könnte seine Existenz bedrohen. Zugleich erwarten knapp zwei Drittel, in den kommenden zwölf Monaten Ziel von solchen Angriffen zu werden. 206 Milliarden Euro Schaden sei den Unternehmen in Deutschland in den vergangenen zwölf Monaten durch Wirtschaftskriminalität entstanden, davon rund 150 Milliarden Euro durch Cyberattacken. (Red.)