In Sachen IT-Sicherheit steht ein hochaktuelles Thema im Fokus: effektives und zukunftsorientiertes Zugriffsmanagement. Warum? Weil die meisten Netzwerkangriffe auf Privilegienmissbrauch zurückzuführen sind, sei es im Zusammenhang mit verzeichnisintegrierten Konten oder mit lokalen Endgeräten. Unternehmen stehen heute vor der Herausforderung, nicht nur ihre IT-Netzwerke und Daten zu schützen, sondern auch strenge gesetzliche Anforderungen zu erfüllen – und das betrifft nicht nur kritische Infrastrukturen (KRITIS). Hier kommt ein risikobasierter Ansatz ins Spiel, der es ermöglicht, beide Ziele schnell und äußerst effizient zu erreichen.

Im Februar dieses Jahres enthüllte ein Insider dem ARD-Magazin Plusminus eine alarmierende Sicherheitslücke in der deutschen KRITIS-Welt: Unzureichend geschützte Solaranlagen mit 14 Megawatt Leistung in Nordrhein-Westfalen hatten voreingestellte Passwörter, die nie geändert wurden. Der Insider entdeckte hunderte ähnlicher unverschlüsselter Login-Seiten für Steuerungsportale von Wind- und Solarparks im Internet. Experten schätzen, dass europaweit rund 2.500 ungesicherte Solaranlagen mit einer Kapazität von etwa 2,8 Gigawatt existieren. Dieses massive Sicherheitsrisiko öffnet kriminellen Hackern Tür und Tor und könnte schwerwiegende Schäden verursachen. Bereits erfolgreiche Cyber-Angriffe auf Windkraftunternehmen deuten auf die Dringlichkeit der Situation hin, da gezielte Angriffe auf erneuerbare Energieanlagen die Netzstabilität der Stromversorgung gefährden könnten. Dies ist nur eines von vielen Beispielen für Angriffe auf Unternehmen aller Art.

Verschärfte Gesetze sollen Schutzniveau heben

Der Bericht beleuchtet eine bestimmte Branche, aber die Realität zeigt, dass andere Branchen ähnliche Probleme haben. Besonders das Gesundheitswesen und Versorgungsunternehmen sind stark betroffen. Tatsächlich sind heute nahezu alle Unternehmen und Organisationen gefährdet. Selbst Bildungseinrichtungen werden vermehrt angegriffen, obwohl man dort keine wertvollen Daten oder großzügige Lösegeldzahlungen vermuten würde. Nicht zuletzt immer mehr staatlich gelenkte Akteure gehen mit gnadenloser Wucht vor, um Identitäten, Zugangsdaten, digitale IT-/OT-Assets und weitere besonders zu schützende Unternehmenswerte anzugreifen. In den meisten Fällen erweisen sich herkömmliche Verteidigungstechniken als unzureichend.

Gesetzgeber und Verbände haben reagiert und strenge Sicherheitsvorschriften für kritische Infrastrukturen erlassen. Der Kreis der als KRITIS geltenden Unternehmen wurde erheblich erweitert. Viele dieser Vorschriften gelten grundsätzlich für alle Unternehmen. Die wichtigsten Vorgaben zur IT-Sicherheit umfassen die ISO 27001-Norm, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Form der B3S veröffentlicht wurde, die IEC 62443, die sich als international anerkannter Standard für Sicherheit in der Prozess- und Automatisierungsindustrie etabliert hat, sowie die NIS 2-Richtlinie.

Die EU-Richtlinie NIS-2 muss bis Oktober 2024 in nationales Recht umgesetzt werden, in Deutschland durch das IT-Sicherheitsgesetz 3.0. Dies dient dazu, einen zeitgemäßen rechtlichen Rahmen für die zunehmende Digitalisierung und Cyberkriminalität zu schaffen. Unternehmen müssen prüfen, ob die erweiterten Regelungen auch kleine Unternehmen und digitale Plattformen betreffen. Die in den Gesetzen schon früher formulierten Anforderungen an das

Cyber-Risikomanagement, das Business Continuity Management, die Zugangskontrolle, die Authentifizierung und andere Sicherheitsmaßnahmen bleiben bestehen oder werden erweitert. Neu ist die Forderung, die Sicherheit entlang der gesamten Lieferkette zu berücksichtigen, was jedoch bereits im deutschen IT-Sicherheitsgesetz 2.0 festgelegt wurde.

Compliance ist Pflicht – Sicherheit bringt den echten Mehrwert

Unternehmen und Organisationen versuchen jetzt eilig nachzuweisen, dass sie die Vorschriften einhalten. Wenn es um die Art und Weise geht, wie der Zugriff auf Systeme geregelt werden soll, gibt es jedoch oft unterschiedliche Meinungen: Die CISOs (Chief Information Security Officers) und Compliance-Beauftragten bevorzugen oft Ansätze, die sich auf die Einhaltung von Checklisten und gesetzlichen Anforderungen konzentrieren. Ihr Hauptziel ist es, erfolgreiche Audits und die Einhaltung von Vorschriften zu gewährleisten. Die tatsächliche Reduzierung von Risiken spielt dabei eine weniger wichtige Rolle.

Im Gegensatz dazu setzen IT-Sicherheitsteams lieber auf risikobasierte Modelle, bei denen der Fokus auf der Minimierung tatsächlicher Risiken und Bedrohungen durch Cyberangriffe und Datenschutzverletzungen liegt. Allerdings stoßen diese Teams oft auf Widerstand seitens des IT-Managements. Dieses erwartet oft (zu) lange Umsetzungszeiträume von zwei bis drei Jahren und erheblichen Aufwand für derartige Projekte.

Das französische Cybersecurity-Unternehmen Wallix hat jedoch bereits in vielen Fällen bewiesen, dass eine rollenbasierte Zugriffsverwaltung mit einem risikobasierten Sicherheitsmodell in nur zwei bis drei Monaten umgesetzt werden kann – und das mit überschaubarem Aufwand. Der einzige vorbereitende Schritt besteht darin, die Kritikalität aller im Unternehmen genutzten Systeme und gespeicherten Daten sorgfältig zu bewerten. Hierbei können gängige BSI- und ISO-Standards sowie entsprechende Tools hilfreich sein. Expertenberatung hilft dabei, die geeigneten Risikoklassen zu bestimmen und individuelle Konzepte zu entwickeln, die den spezifischen Anforderungen des Unternehmens gerecht werden. Basierend auf der Risikoklasse werden dann spezifische Schutzmaßnahmen festgelegt, um den Sicherheitsbedarf angemessen zu decken.

Eine solide Rollen- und Berechtigungsstruktur ist von entscheidender Bedeutung, um Privileged Access Management (PAM) erfolgreich einzusetzen. In diesem Bereich bietet das Risikoklassenmodell von Wallix unschätzbare Vorteile. Zusätzlich erleichtern praxisorientierte Vorlagen die notwendigen Autorisierungsprozesse erheblich.

Hohe Transparenz und Kontrolle als Bonus

Die Einführung eines risikobasierten Zugriffsmanagementsystems bietet zahlreiche Vorteile. Unternehmen können damit die Zugriffe auf ihre Systeme gezielt steuern und überwachen. Dies verschafft ihnen eine deutlich verbesserte Kontrolle über den Zugang zu ihren Ressourcen, insbesondere wenn externe Mitarbeiter und Dienstleister involviert sind. Das System schließt bestehende Wissenslücken über Zugriffe, indem es Informationen darüber bereitstellt, wer zu welchem Zeitpunkt auf welche Daten zugegriffen hat. Dies ist ein entscheidender Faktor im kontinuierlichen Verbesserungsprozess eines Information Security Management Systems (ISMS).

Darüber hinaus bietet die Implementierung eines risikobasierten Zugriffsmanagementsystems klare Vorteile. Sie vereinfacht Geschäftsprozesse und ermöglicht transparente Audit-Trails, die den Zugang zu internen Systemen rückverfolgbar machen. Wallix unterstützt maßgeschneiderte Zugangsregelungen, das effektive Management von Risiken und die Einteilung in Risikoklassen, wodurch eine rasche Umsetzung der erforderlichen Abläufe ermöglicht wird. Damit wird die Sicherheitsinfrastruktur von Unternehmen auf ein neues Niveau gehoben und schafft die Grundlage für effiziente, zukunftssichere Geschäftsabläufe.

CISOs und IT-Sicherheitsteams ins gleiche Boot holen

Die Konflikte zwischen CISOs (Chief Information Security Officers) und IT-Teams beim Zugriffsmanagement können die Unternehmensressourcen belasten. Ein risikobasiertes Zugriffsmanagementsystem hat jedoch das Potenzial, beide Seiten zu überzeugen. Dies liegt daran, dass die Umsetzung schnell und kostengünstig ist, was die finanziellen Bedenken der CISOs löst. Zusätzlich erfüllt die Implementierung eines solchen Systems mehrere wichtige Compliance-Anforderungen. Wallix legt besonderen Wert auf das Zugriffsmanagement im gesamten IT-Bereich, insbesondere auf die Sicherung privilegierter Konten und sensibler Zugangsdaten. Dadurch gehen Compliance und IT-Sicherheit Hand in Hand, und CISOs sowie IT-Teams arbeiten gemeinsam an denselben Zielen.

Es ist wichtig zu beachten, dass ein risikobasiertes Zugriffsmanagementsystem kontinuierlich aktualisiert werden muss, da sich die Risiken ständig ändern. Um sicherzustellen, dass das System kontinuierlich

wirksam ist und den aktuellen Anforderungen entspricht, ist eine regelmäßige Überwachung und Überprüfung unerlässlich. Die Anpassungen sind jedoch nicht allzu aufwendig – zumal mit den angebotenen Tools – solange die ursprüngliche Klassifizierung sorgfältig durchgeführt wurde.

Insgesamt stellt der risikobasierte Ansatz im Zugriffsmanagement eine äußerst wirkungsvolle Strategie dar, mit der Unternehmen nicht nur die Einhaltung von Compliance-Anforderungen sicherstellen, sondern auch ihre Systeme effektiv schützen können, um den ständig wachsenden digitalen Bedrohungen standzuhalten. Wallix hat eindrucksvoll gezeigt, dass die Implementierung dieses Ansatzes nur geringen Aufwand erfordert und gleichzeitig immense Vorteile bietet. Es ist die Investition wert, um Sicherheit und Compliance im Unternehmen zu gewährleisten.

Stefan Rabben, *Area Sales Director DACH & Eastern Europe bei Wallix*

Warum Wallix?

Wallix verfolgt die ehrgeizige Mission, das Sicherheitsniveau von Unternehmen und deren Systemen durch innovative Zugriffsmanagement-Lösungen auf ein neues Level zu heben.

Der risikobasierte Ansatz ermöglicht die präzise Festlegung von Zugriffs- und Interaktionsregeln, die auf Risikobewertungen und Schutzbedarfsanalysen basieren. Dies erlaubt die gezielte Beschränkung von Zugriffen auf besonders risikoreiche Systeme, um potenzielle Bedrohungen zu minimieren.

Als enger Partner von Information Security Management Systemen (ISMS) trägt Wallix zur Erfüllung von Compliance-Anforderungen bei, insbesondere im Rahmen des ISO 27001 Frameworks für Zugriffskontrollen.

Durch die systematische Klassifizierung von Unternehmenssystemen gemäß ihrer kritischen Bedeutung und die individuelle Zuordnung von Risikoklassen bietet Wallix maßgeschneiderte Lösungen, um Zugriffsmanagement effizient umzusetzen und ein hohes Maß an Sicherheit zu gewährleisten. Mit Wallix lassen sich Unternehmensdaten optimal schützen und gleichzeitig die regulatorischen Vorgaben erfüllen.