Cyber-Attacke aus den eigenen Reihen

Wie Sie mit zentralen Zugangsprotokollen Ihre Sicherheit erhöhen

(BS/Thomas Buch) "Die Bundesregierung hat eine Serie von Cyber-Angriffen auf deutsche Behörden und Ministerien bestätigt." Stockte auch Ihnen der Atem bei dieser Meldung im Mai 2022? Die Tagesschau berichtete damals über Hackerangriffe auf die Webseiten von Bundesbehörden und Ministerien. Eine russische Gruppe bekannte sich zu den Taten. Schaden sei nicht entstanden. Glück gehabt?

Im Juli 2021 verlief ein Angriff weniger glimpflich: Da wurde der Landkreis Anhalt-Bitterfeld durch eine Cyber-Attacke so weit lahmgelegt, dass die Auszahlung von Sozial- und Unterhaltsleistungen über Wochen nicht möglich war. Vom Daten-Phishing, das sensible Daten abgreift, bis zum Hackerangriff, der alle Systeme lahmlegt: Attacken auf Verwaltungen und Kritischen Infrastrukturen nehmen zu. 2021 stieg die Anzahl der Phishing-Attacken um 200 Prozent. Der Krieg in der Ukraine hat die Bedrohungslage verschärft.

Doch während die öffentliche Verwaltung ihre IT nach außen mit Natodraht und Kryptonite-Schlössern abschirmt, haben Angriffe aus den eigenen Reihen oft ein leichtes Spiel. Dabei zählen Insider-Attacken zu den größten Gefährdungen für eine Organisation. Schätzungen gehen von 60 Prozent aus. Die Dunkelziffer ist hoch. Die interne IT-Infrastruktur birgt also ein immenses Risiko.

Wenn die Bedrohung aus dem Innern kommt. Foto: BS/Valery Brozhinsky, shutterstock

Thomas Buch ist Senior Manager Sales bei OPITZ CONSULTING und betreut seit über 20 Jahren Kunden im Bereich der Öffentlichen Auftraggeber in Themen der Digitalisierung, Modernisierung und IT-Sicherheit.

Foto: BS/OPITZ CONSULTING

Die Bedrohung im eigenen Haus

"Warum sollten meine eigenen Leute so etwas tun?", fragen Sie sich vielleicht. Tatsächlich kann es dafür unterschiedlichste Gründe geben: Beschäftigte, die sich ungerecht behandelt fühlen und Ihrer Organisation bewusst schaden wollen, oder Mitarbeitende, die von kriminellen Dritten angeworben werden, können die Ursache sein. Die meisten Bedrohungen aber entstehen aus Unwissenheit, Fahrlässigkeit oder Langeweile: Eine Verwaltungskraft, die ohne nachzudenken auf einen Link klickt. Eine Sachbearbeiterin, die einen privaten USB-Stick benutzt. Ein unzureichend geschulter Administrator, der sich an einer Sicherheitslücke ausprobiert.

Die Folgen möchte niemand erleben: Ein Sicherheitsvorfall bringt Ihrer Organisation nicht nur negative Schlagzeilen, sondern Sie womöglich auf die Anklagebank. Denn Sicherheitsabteilungen müssen Zugriffe auf schützenswerte Daten und Systeme jederzeit nachweisen können. Der sorgsame Umgang mit personenbezogenen Daten ist also kein Nice-to-have. Er ist gesetzlich verpflichtend und fester Bestandteil eines Risk- und Business Continuity Managements (BCM).

Wie aber kommen Sie Mitarbeitenden auf die Spur, die bewusst oder unbewusst dafür gesorgt haben, dass interne Daten das Haus verlassen konnten? Wie finden Sie heraus, wer Daten manipuliert oder gelöscht hat? Und wie können Sie beweisen, dass kein strukturelles Problem vorliegt, sondern Einzelpersonen oder Kriminelle für einen Sicherheitsvorfall verantwortlich sind?

Systeme als Sicherheitsrisiko

Was tun Sie nicht alles! Tag für Tag bemühen sich IT-Abteilungen, Zugriffe zu protokollieren und Sicherheitslücken zu schließen. Das Problem: Die Systeme entwickeln sich immer schneller weiter. Dabei werden sie zunehmend verteilter und komplexer. Die Protokollierung jedoch erfolgt meist individuell für jede Anwendung, wird einfach ins Dateisystem geschrieben und im Zweifel gar nicht abgebildet. Überwachungslücken sind damit vorprogrammiert.

Die Lösung: ein zentraler Protokollserver

Die IT-Fachleute von OPITZ CONSULTING beschäftigen sich seit 2018 mit der Zugriffskontrolle in Organisationen mit höchsten Sicherheitsanforderungen. Dafür haben sie jetzt einen Protokollserver entwickelt, mit dem sie Zugriffe auf alle Systeme einheitlich erfassen sowie integritätsgeschützt und verschlüsselt speichern können: gemäß BSI-IT-Grundschutz, ISO/IEC 27001 und EU-DSGVO-Kompendium für alle Systeme. So werden Leaks nachverfolgbar und illegale Eingriffe entdeckt, bevor sie Schaden anrichten. Anforderungen werden an einer Stelle definiert und von hier für die gesamte Organisation ausgerollt. Es gibt also weder Matching-Probleme noch Überwachungslücken.

OPITZ CONSULTING bietet eintägige Workshops an, um Ihre individuellen Vorteile durch den OC | Protokollserver zu evaluieren.

Unter www.opitz-consulting.com/protokollserver gelangen Sie zur Anmeldung und weiterführenden Informationen zu den Workshops.