Interview zu IT-Security: Manfred Lackner, PROFI AG

„Konzentration auf die wesentlichen Risiken“

In Zeiten des übergreifenden Cloud-Einsatzes und der Einbeziehung von „Internet of Things“ (IoT) in die bestehende IT-Infrastruktur kommen auf die Verantwortlichen in den Unternehmen neue Herausforderungen im Bereich IT-Security zu. Manfred Lackner, Vorstandsvorsitzender der PROFI AG, skizziert im Interview mit dem Midrange Magazin (MM) vielversprechende Lösungsansätze.

MM: Nur ein umfassender Ansatz kann die Sicherheitsprobleme eines Unternehmens in den Griff bekommen. Was empfehlen Sie einem Mittelständler?

Lackner: Zunächst muss er sich im Klaren darüber sein, wo die wesentlichen individuellen Risiken für sein Unternehmen liegen. Neben verschiedenen Maßnahmen zur breiten Grundsicherung sollte er seine Bemühungen bezüglich der IT-Sicherheit auf diese Kernrisiken fokussieren. Das kann für den einen die Intellectual Property seiner Konstruktionspläne sein, für den anderen seine Webshop Plattform und für einen dritten eine hochsensible Kunden-Datenbank.

MM: Wie kommen KMUs an genügend qualifiziertes Personal?

Lackner: Das ist aktuell kein einfaches Thema. Die gut ausgebildeten und erfahrenen Fachleute sind begehrt, und die interne Ausbildung kann sich sehr aufwändig gestalten. Aber das kann sich durchaus lohnen, denn wenn ein Mitarbeiter mit der Informationssicherheit im Unternehmen langfristig wächst, kann er die kritischen Anforderungen an die Geschäftsprozesse am besten verstehen und deren Einhaltung gewährleisten. Aufgaben, die hohes Expertenwissen in speziellen Bereichen erfordern, werden dabei am besten nach außen gegeben. Die Governance muss aber immer interne Aufgabe bleiben.

MM: Welche Besonderheiten birgt das Konzept eines Advanced Cyber Defense Center – kurz ACDC?

Lackner: Das Besondere an diesem Ansatz ist die Use-Case-fokussierte Herangehensweise. SIEM-Systeme sind bislang häufig in Betrieb genommen worden, ohne dass vorher ein klares Konzept bezüglich der tatsächlich kritischen Anwendungsfälle existierte. Die Management-Lösung Security Information and Event Management, kurz als SIEM bezeichnet, basiert auf unternehmensspezifischen Anforderungen – also auf klaren und umfassenden Definitionen, welche Ereignisse sicherheitsrelevant sind und wie mit welcher Priorität darauf zu reagieren ist. Sie zielt darauf ab, anhand eines Regelwerks kontinuierlich die Standards für Sicherheit, Compliance und Qualität des IT-Betriebs zu verbessern. ACDC bietet die Entdeckung und Alarmierung von Vorfällen, die im Vorfeld ausführlich und maßgeschneidert designed worden sind. Um auch wirklich nur für den Kunden relevante Use Cases aufzunehmen arbeiten wir in diesem Umfeld mit den Experten der KPMG zusammen, die dazu aus einem reichen Erfahrungsschatz schöpfen können.

MM: Wie kann ein typischer „Mittelständler“ sich die ACDC-Lösung zunutze machen?

Lackner: 80 Prozent der Arbeit findet im Vorfeld statt, bevor irgendetwas Technisches passiert: Gemeinsam mit dem Kunden werden die für ihn relevanten Use Cases erarbeitet und ausformuliert. Darauf basierend findet die Übersetzung in die technologischen Anforderungen sowie das Design der einzelnen Alarmpläne statt. Die Implementierung selbst geht dann relativ schnell – und der Kunde muss sich weder um Hardware noch um Lizenzen kümmern.

MM: Wer hilft einem Unternehmen bei der Bestimmung des Status quo?

Lackner: Für eine erste Selbsteinschätzung gibt es verschiedene Online-Fragebögen. Einen größeren Detaillierungsgrad erreicht man beispielsweise durch ein von uns durchgeführtes Security Assessment, das dem Kunden auf Basis einer IST-Aufnahme priorisierte Empfehlungen und Verbesserungsvorschläge bietet. Wenn man sich zum Beispiel wegen externer Anforderungen nach einem Standard wie ISO 27001 zertifizieren muss, so arbeiten wir mit erfahrenen Partnern in diesem Bereich zusammen.

MM: Warum erweist es sich in der Praxis als eine gute Lösung, ein Security Operations Center (SOC) von einem Dienstleister betreiben zu lassen?

Lackner: Wichtigster Grund ist sicherlich der Aufwand, der mit einem internen

Manfred Lackner, Vorstandsvorsitzender der PROFI AG: „IoT hat schon jetzt realen Impact auf alle Unternehmen. Der Einsatz von IoT-Devices im Unternehmensnetz muss klar geregelt sein, um das Gefährdungspotenzial so gering wie möglich zu halten." Quelle: Profi AG

SOC verbunden ist: Neben einer hohen Expertise benötigt man ausreichend Personal, um einen 24/7-Betrieb aufrecht zu erhalten. Das ist für viele Mittelständler schlicht nicht effizient abbildbar. Die internen Ressourcen sollten sich eher mit der individuellen Bearbeitung der im SOC identifizierten und qualifizierten Findings und Incidents beschäftigen, als ihre Zeit mit Triage, False Positives und dem Tuning des Überwachungssystems zu verbringen.

MM: Wie muss ein „externes SOC" konzipiert sein, um auf die jeweiligen Besonderheiten der IT-Sicherheit eines Unternehmens eingehen zu können?

Lackner: Idealerweise schafft es die Balance zwischen professionellem, prozessorientierter Serviceleistung und individuellem Eingehen auf den Kunden.

MM: Welche zusätzlichen Sicherheitsanforderungen kommen auf, wenn sich ein Unternehmen mit Inhouse-IT einer zusätzlichen externen Cloud-Nutzung verschrieben hat?

Lackner: Grundsätzlich spricht aus Sicht der IT-Sicherheit wenig gegen eine Cloud-Nutzung, solange sie denselben Sicherheitsrichtlinien wie eine OnPremise-Lösung folgt. Diese Richtlinien müssen natürlich erst einmal definiert sein. Das ist die Grundlage des IT-Security Managements. Besonders interessant bei Cloud-Entscheidungen sind aber die Regularien des Datenschutzes, besonders mit der neuen EU General Data Protection Regulation. Diese Verordnung regelt die Rechtsgrundlagen der Datenverarbeitung, die Rechte der Betroffenen und die Pflichten der Verantwortlichen. Darüber hinaus muss das Vertragswerk im Detail durchleuchtet werden, zum Beispiel auf die Möglichkeiten zur Datenrückführung bei Vertragskündigung oder Insolvenz des Anbieters.

MM: Wie muss ein Sicherheitskonzept aufgesetzt sein, um künftig auch für das Zusammenspiel mit dem Internet of Things – IoT – gerüstet zu sein?

Lackner: IoT hat schon jetzt realen Impact auf alle Unternehmen. Der Einsatz von IoT-Devices im Unternehmensnetz muss klar geregelt sein, um das Gefährdungspotenzial so gering wie möglich zu halten. Häufig handelt es sich um Embedded Devices, die nur sehr schlechten Schutz vor neuen Angriffen haben, weshalb sie von sensiblen Systemen zu isolieren sind. Was auf keinen Fall passieren sollte ist das unkontrollierte Integrieren von IoT Devices in bestehende Umgebungen. Die jüngste Vergangenheit mit großflächigen Angriffen auf Telekom-Router und übernommene IP-Kameras hat gezeigt, dass schlecht geschützte Geräte eine Gefahr darstellen, da sie für massive „Distributed Denial of Service"-Angriffe missbraucht werden können. Denial of Service, als DoS abgekürzt, bezeichnet die Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte. In der Regel als Folge einer Überlastung von Infrastruktursystemen. Dies kann durch einen absichtlichen Angriff auf einen Server, einen Rechner oder sonstige Komponenten in einem Datennetz verursacht werden. Wird die Überlastung von einer größeren Anzahl anderer Systeme verursacht, so wird von Distributed Denial of Service – DDoS – gesprochen. Dementsprechend sollte man sich gegen solche Angriffe dringend schützen, bevor diese das eigene Unternehmen treffen.

MM: Welche Themen stellen Sie auf der CeBIT 2017 dem Publikum vor?

Lackner: Unsere Experten zeigen in praktischen Beispielen Nutzen und Vorteile der Managed SIEM- und ACDC-Lösungen auf. An unserem Stand in Halle 2 bei IBM erfahren Interessierte alles rund um diese innovativen Lösungen. Eines ist klar: SIEM-Systeme sind eine sinnvolle Ergänzung zu jedem Security-Konzept. Aber ihr Einsatz muss von Anfang an strategisch geplant sein. Deshalb demonstrieren die Spezialisten der PROFI anhand von Business Cases, worauf zu achten ist, um SIEM-Systeme zielgerichtet und risikobasiert bereitzustellen.

Rainer Huttenloher ■