

Wenn Peter fehlt

Physische Sicherheit ist in den meisten Organisationen nicht vergessen – aber oft wird nicht so genau hingeschaut.

von Martin Furrer, Senior Consultant, Swiss Infosec AG

Es gibt eine Kategorie von Sicherheitsrisiken, die in keinem Dashboard erscheint und kein Penetrationstest aufdeckt. Sie sitzt im Kopf von Peter, dem Leiter Facility, der seit zwölf Jahren weiss, dass die Badge-Berechtigungen der externen Reinigungsfirma seit dem letzten Vertragswechsel nicht sauber nachgeführt wurden, und der das nie dokumentiert hat, weil es niemand gefordert hat.

Es bleibt ein Zutrittssystem, das formal korrekt aussieht, aber eine Lücke hat, von der niemand mehr weiss – weil Peter seit anderthalb Jahren nicht mehr in dieser Funktion ist. Das begegnet uns regelmässig.

Gewachsen, bewährt und dabei kaum verstanden

Physische Sicherheit funktioniert in vielen Organisationen, weil die Menschen oft die gleichen geblieben sind. Weil sich jemand an etwas erinnert hat, das nirgends dokumentiert war. Zutrittskonzepte aus längst abgeschlossenen Projekten. Schlüsselverwaltung, die auf dem Wissen einer Person basiert, die das Unternehmen verlassen hat. Externe Dienstleister, deren Zugangsberechtigung auf Vertrauensbasis läuft. Das ist nicht zwingend Nachlässigkeit, es ist das Ergebnis davon, dass Sicherheitsstrukturen im Alltag Kompromisse erfordern.

Was passiert, wenn die Bedingungen sich ändern

Ein Unternehmen, gut aufgestellt in der Informationssicherheit: SOC, regelmässige Audits, ausgereifte Incident Response. Gleichzeitig ein Zutrittssystem mit nie bereinigten Berechtigungen und veralteten Schutzzonen. An einem gewöhnlichen Dienstagmorgen kommt ein externer Techniker, dessen Zugangskarte längst hätte deaktiviert sein sollen, es gibt keinen Prozess dafür. Er gelangt in eine Grauzone, in der sich Netzwerk-

infrastruktur befindet, die nie explizit als schützenswert ausgewiesen wurde. Ein falscher Handgriff, eine kurze Unterbrechung.

Systeme zeigen auffälliges Verhalten. Das Monitoring reagiert und beginnt, wie immer, im Netzwerk. Es dauert über eine Stunde, bis klar wird, dass die Ursache physischer Natur ist. Die Wiederherstellung ist komplizierter als erwartet, weil niemand eine klare Übersicht hatte, welche physische Infrastruktur welche digitalen Systeme trägt.

Die Informationssicherheit hat funktioniert – das Problem lag davor

Monitoring und Incident Response haben funktioniert. Das Problem lag ausserhalb des Wahrnehmungsbereichs: in der physischen Realität des Gebäudes, in gewachsenen Zutrittsprozessen, in der fehlenden Verbindung zwischen Konzept und Betriebsrealität. Physische Sicherheit ist Facility-Thema, Informationssicherheit ist IT-Thema – dazwischen gibt es selten ein gemeinsames Risikobild. Dabei sind Zutrittskontrolle, Alarmierung und Videoüberwachung längst selbst digitale Systeme mit Konfigurationen und Schnittstellen, die selten vollständig dokumentiert sind.

Der Mensch und warum die einseitige Betrachtung zu kurz greift

Der menschliche Faktor erscheint in der Sicherheitsdiskussion meistens als Problem. Das stimmt, Menschen umgehen Prozesse, die im Alltag unpraktisch sind. Aber es ist fast immer auch ein Mensch, der in einer unklaren Situation das Richtige tut: der nachfragt, eine Abweichung meldet, erkennt, dass etwas nicht stimmt. Nicht weil ein System Alarm schlägt, sondern weil er Erfahrung hat. Sicherheitskonzepte, die den Menschen primär als Risikofaktor behandeln, verpassen

diese Ressource. Was funktioniert, sind Strukturen, in denen Menschen wissen, warum eine Massnahme sinnvoll ist – und in denen implizites Wissen wie das von Peter festgehalten wird, bevor es verloren geht.

Was das in der Praxis bedeutet

Es braucht keine Megaprojekte, sondern ehrliche Antworten auf unbequeme Fragen: Welche physischen Sicherheitsstrukturen funktionieren, weil sie gut aufgebaut sind und welche, weil bestimmte Personen sie stillschweigend am Laufen halten? Wo gibt es implizites Wissen, das nie dokumentiert wurde? Welche physischen Abhängigkeiten der IT waren nie Teil einer integrierten Risikobetrachtung? Und wo haben sich Abweichungen als Normalzustand eingeschlichen?

Diese Fragen lassen sich nicht durch ein Audit beantworten, das Konzepte gegen eine Checkliste prüft. Sie erfordern die Bereitschaft, zwischen dokumentierter Sicherheit und wirksamer Sicherheit zu unterscheiden. Das ist nicht immer dasselbe. Physische und digitale Sicherheit als zusammenhängendes System zu verstehen, bedeutet anzufangen, dort hinzuschauen, wo das eigene Sicherheitskonzept bisher schlicht nicht ausgerichtet war.

DIE INHALTLICHE VERANTWORTUNG FÜR DEN ARTIKEL LIEGT BEI SWISS INFOSEC AG.

DER AUTOR

Martin Furrer, Senior Consultant bei der Swiss Infosec AG, fokussiert auf physische Sicherheit, Informationssicherheit, Riskmanagement und BCM. Nebst langjähriger Erfahrung verfügt er über einen CAS in GRC der Hochschule Luzern. Er kann sicherheitsrelevante Anforderungen in praxistaugliche Strukturen und Prozesse übersetzen.