Integraler Unternehmensschutz – Security Scouts zur Früherkennung von Unternehmensrisiken

Geschrieben von Joshua Bucheli, Forscher und Redakteur, in Zusammenarbeit mit Chris Eckert, CEO der Swiss Business Protection AG und Peter Kosel, Gründer von cyberunity

«Wenn du dich und den Feind kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten.»
– Sun Tzu

In der heutigen Unternehmenswelt, in der digitale Innovationen und Cyber-Bedrohungen mit halsbrecherischer Geschwindigkeit voranschreiten, geht allzu leicht vergessen, dass 'Sicherheit' mit einem grossen 'S' – auch Integraler Unternehmensschutz (IUS) genannt – eine ganzheitliche Disziplin ist, die über die reine Cybersicherheit hinausgeht.

Die Verteidigung von Cloud-Systemen und die Vorbereitung der Verschlüsselung auf das Quantenzeitalter sind wohl wichtige Elemente der Unternehmenssicherheit des 21. Jahrhunderts, aber sie ersetzen keineswegs die Notwendigkeit umfassenderer Sicherheitsmassnahmen innerhalb eines Unternehmens.

Jedes Unternehmen hat Vermögenswerte, die geschützt werden müssen – **die sprichwörtlichen 'Kronjuwelen'** – und alle Entscheidungen sollten die Sicherheit dieser Vermögenswerte berücksichtigen. Das Problem ist, dass in der Praxis oft Schwachstellen offengelassen werden und Fehltritte in der Sicherheit eher kurzfristig behoben oder gar vertuscht als vermieden werden.

Diese fehlende 'Awareness' macht Unternehmen anfällig für Ausbeutung und erschwert ihnen die Erkennung und Abwehr von Bedrohungen - denn wie kann man etwas schützen, wenn man nicht weiss, dass es geschützt werden muss?

Wie Chris Eckert, CEO der Swiss Business Protection AG, Studiengangsleiter des CAS Business Protection an der HWZ und ehemaliger Fahndungschef der Kantonspolizei Zürich kürzlich in einem

Interview betont, geht es beim Integralen Unternehmensschutz darum, reaktive Schadensbegrenzung mit proaktiver Aufklärung sowie wirkungsvollen Massnahmen, Threat Awareness und Training zu ergänzen.

Wo steht das Thema Integraler Unternehmensschutz heute?

Während seinen Mandaten als externer CISO und CSO konnte Chris aus erster Hand beobachten, wie unterentwickelte IUS-Strategien und eine geringe 'Awareness' Unternehmen in Gefahr brachten:

Er sah, wie Phishing-E-Mails, als legitime Korrespondenz des CEO getarnt, Mitarbeiter dazu brachten, grosse Summen an Firmengeldern an Dritte zu überweisen. Er hatte mit Mitarbeitern zu tun, die unbekannte USB-Laufwerke in ihre Firmencomputer einsteckten und damit die Cybersicherheit des Unternehmens kompromittierten. Er wurde sogar Zeuge eines Falles, in dem ein Flipchart nach einem strategischen Meeting liegen gelassen und nach Feierabend von einer unbefugten Person fotografiert wurde.

Man kann mit Sicherheit sagen, dass heute das Sicherheitsparadigma eher reaktiv als proaktiv ist. Unternehmensverantwortliche schenken den sogenannten 'Kronjuwelen' immer noch nur begrenzte Aufmerksamkeit, und allzu oft wird das Thema Sicherheit auf die IT-Abteilung abgeschoben, anstatt in der Verantwortung der Manager zu bleiben.

Zugegebenermassen sind bestimmte Branchen, die einer umfangreichen externen Regulierung unterliegen und regelmässigen Audits unterworfen sind, wie Banken, die Pharmaindustrie und der Energiesektor, in Bezug auf Integrale Unternehmenssicherheit vielleicht schon ein wenig weiter als andere.

Auch die Gesundheitsbranche bemüht sich neuerdings die Bedeutsamkeit des IUS zu erkennen. In Krankenhäusern, in denen kontrollierte Substanzen und sensible Patientendaten vor Ort gelagert werden, ist die Notwendigkeit, den Zugang zu gesperrten Bereichen (sowohl analog als auch digital) zu verwalten und zwischen autorisiertem Personal und jedem beliebigen Laborkittel zu unterscheiden, einigermassen etabliert. Dennoch besteht auch hier ein erhebliches Verbesserungspotenzial was IUS anbelangt.

«Insgesamt steckt IUS noch in den Kinderschuhen. Jeder denkt, er sei nicht wichtig genug, um ein lohnendes Angriffsziel darzustellen… Dies ist ein entscheidender Fehler. Von grossen internationalen Konzernen bis hin zu kleinen lokalen Unternehmen, jeder kann zum Opfer werden. Und doch scheint IUS immer erst dann auf dem Radar von Unternehmen aufzutauchen, wenn sie bereits Opfer von Betrug oder Spionage geworden sind.»

Es ist daher zwingend erforderlich, dass Unternehmen und Manager eine ganzheitlichere Denkweise in Bezug auf die Unternehmenssicherheit entwickeln, anstatt sich auf IT-Spezialisten zu verlassen, die erst dann Schadensbegrenzung betreiben, wenn riskante Entscheidungen und Verfahren zu unerfreulichen Konsequenzen geführt haben.

In diesem Zusammenhang hebt Chris einen interessanten Punkt hervor, nämlich Sicherheit als Vermögenswert statt als Kostenfaktor zu sehen:

«Im Moment wird Sicherheit immer noch als Geschäftskosten gesehen, bei denen es keine Preise zu gewinnen gibt. Aber die Einstellung von Personen, die für Sicherheit am Arbeitsplatz sorgen können, muss nicht zwingend als Belastung betrachtet werden. Mit ein wenig Einfallsreichtum kann es sogar in einen Ruf verwandelt werden, der Partnerschaften begünstigt und Kunden anzieht.»

Security Scouts – Gefragte Fähigkeiten und Ausbildungen:

Was Unternehmen vor allem brauchen, sind sogenannte 'Security Scouts' – Personen, die dabei helfen können 1) sich ihrer Vermögenswerte bewusst zu werden, 2) Bedrohungen, denen diese ausgesetzt sind (sowohl Digital- als auch Analog) aufzuklären und 3) Sicherheitsmassnahmen zum Schutz dieser Vermögenswerte in alle Ebenen der Unternehmensaktivitäten zu integrieren.

Diese Scouts werden aus unterschiedlichsten Bereichen kommen, von Informatikern, Elektronikern, Haustechnikern, Wirtschaftsinformatikern und Wirtschaftsingenieuren bis hin zu Rechtsexperten und Fachleuten für Wirtschaftsrecht, Wirtschaftskriminalität, Finanzen, CSR, Risk, Governance, und Compliance.

Zu diesem letzten Punkt ein Wort der Warnung von Chris: «Obwohl es von Vorteil ist, wäre es wichtig, dass Personen mit diesen Hintergründen ein übermässiges Vertrauen in theoretisches Wissen vermeiden und ihre praktischen Fähigkeiten sowie Erfahrungen in Bewerbungen betonen.»

Die Kunst liegt darin, diese Fachleute zu einem umfassenden Team zu vereinen, welches das Sicherheitsbewusstsein des Unternehmens stärkt. So werden zum Beispiel Kriminalisten und Elektroniker benötigt, um das Unternehmen und seine Hardware nach Wanzen zu durchsuchen, Informatiker und Bauingenieure, um Baupläne auf strategische Schwachstellen zu analysieren, und Risikomanager, um die Mitarbeiter im verantwortungsvollen Umgang mit dem Firmenvermögen bei ihren täglichen Aufgaben zu schulen.

Auf operativer Ebene wird ein solcher Mentalitätswandel hin zu einem ganzheitlichen und proaktiven Ansatz für die Unternehmenssicherheit wahrscheinlich (zumindest teilweise) als Top-Down Umstellung erfolgen, was Personen mit Erfahrung in C-Suite-Positionen wie CISOs, CIOs, CEOs und insbesondere CSOs oder COOs absolut notwendig macht.

Erfahrene Manager, vorzugsweise solche, die mit Prozess-, Betriebs- und vor allem Business-Continuity-Management vertraut sind, werden für Unternehmen, die auf der Suche nach Security Scouts sind, ebenfalls ein grosser Gewinn sein.

Zurzeit gibt es noch keinen einheitlichen Studiengang für angehende IUS-Profis. Mit Zertifikaten und Qualifikationen wie dem CAS Business Protection der HWZ erhalten ambitionierte Persönlichkeiten jedoch ein solides Fundament für ganzheitliche Ansätze der Unternehmenssicherheit.

Personality:

Neben dem technischen Know-how gibt es einige wichtige Persönlichkeitsmerkmale, die zum Erfolg im Security Scouting beitragen werden. Neugierde, sehr rasches Querdenken, Pragmatismus, starke analytische Fähigkeiten und eine detektivische Ader sind entscheidend für eine erfolgreiche Karriere im Bereich IUS. Zusätzlich sind Fähigkeiten der sofortigen praktischen Umsetzbarkeit sowie die Gabe, sich in einen Gegner hinein zu versetzen, zunehmend wichtig.

«Wir brauchen Personen mit einem Talent für ganzheitliche Problemlösungen, die Herausforderungen und Bedrohungen beharrlich aus allen Blickwinkeln betrachten, und wir brauchen Querdenker mit dem Mut, Vorgesetzte herauszufordern, wenn sie sehen, dass IUS Best Practices nicht eingehalten werden», sagt Chris. «Glaube wenig, hinterfrage alles, denke selbst und ständig» ist ein Credo, dass einem in einer solchen Funktion erfolgreich machen wird.

IUS ist per Definition eine Teamleistung – die Bedrohungen ändern sich ständig und kein Einzelner wird alle notwendigen Befähigungen mitbringen, um eine undurchdringliche Unternehmens-sicherheit zu gewährleisten. Es ist daher entscheidend, dass angehende IUS-Security Scouts in der Lage sind, sich in einer dynamischen Umgebung zu integrieren und gut mit anderen zu vernetzen – sie müssen sich mit Personen aus unterschiedlichem Hintergrund zusammentun, um Schwachstellen in einem Unternehmen aus allen Winkeln zu identifizieren und zu beheben.

Peter Kosel Founder und Talent Community Manager der cyberunity AG weist zusammenfassend darauf hin, dass die Zukunft der Unternehmenssicherheit im Wesentlichen von drei Entwicklungen abhängt: Erstens müssen Unternehmen und ihre Führungskräfte ein Bewusstsein für integrale Unternehmenssicherheit entwickeln. Zweitens ist der vorausschauende Aufbau von Talentpools mit unterschiedlichen, dynamischen und kompetenten Individuen gefragt (im Gegensatz zu althergebrachter Gewinnung von Mitarbeitenden, die meist erst dann startet, wenn eine Vakanz dringend zu besetzen ist – KNOW YOUR TALENTS). Drittens müssen diese unterschiedlichen, dynamischen und kompetenten Individuen ihren Mehrwert für die Unternehmen erkennen und aktiv in Erscheinung treten.

Interessenten für den CAS integrale Unternehmenssicherheit erhalten unter nachfolgendem Link weiterführende Informationen und können sich zu der im Juni 2021 startenden Weiterbildung anmelden:

Anmeldung CAS Business Protection