BILD: APINAN / ADOBESTOCK.COM

Der Feind im eigenen Büro

Wer sich vor Cyberbedrohungen schützen will, blickt in der Regel über seine Festungsmauern nach draussen. Aber nicht alle Gefahren drohen von ausserhalb – manche lauern im eigenen Netzwerk. Wie man mit diesen Insider Threats umgeht, sagen Experten von Boll, Check Point, Eset, G Data, Infinigate, Infoguard, Oneconsult und Trend Micro. Interviews: Coen Kaat

Christopher Cantieni
Head of Technical Services, Infinigate Schweiz

Was macht Insider Threats zu einer so grossen Bedrohung?
Christopher Cantieni: Ein Insider ist in den meisten Fällen keine Person mit bösen Absichten, die sich Zugang zu einem Unternehmen verschafft, sondern Mitarbeitende, die bereits Zugang zum Unternehmen haben. Aufgrund einer Unachtsamkeit werden unbewusst vertrauliche Informationen preisgegeben oder ein Mitarbeiter wird Opfer eines Social-Engineering-Angriffs. Solche Angriffe bleiben meist über längere Zeit unbemerkt, da der Mitarbeiter es entweder selbst nicht bemerkt oder Angst hat, den Vorfall zu melden. Zeit ist bei Cyberangriffen ein kritischer Faktor. Je länger ein Angriff unbemerkt bleibt, desto grösser ist der Schaden.

Wie gross ist das Risiko für Schweizer Unternehmen?
Das kann man so nicht generell beantworten. Die Schweiz ist jedoch ein KMU-Land, und die Erfahrungen zeigen, dass KMUs weniger als Grossunternehmen gewillt sind, Geld für IT-Security und die Sensibilisierung ihrer Mitarbeitenden auszugeben. Somit lässt sich annehmen, dass das Risiko für Schweizer Unternehmen relativ hoch ist.

Wie unterscheidet man beabsichtigte von unbeabsichtigten Vorfällen? Packt man beide Fälle gleich an?
Wie gesagt, geschehen die meisten Vorfälle unbeabsichtigt. Also sprechen wir eigentlich von einem Unfall, den man nicht oder nur schwer voraussehen kann. Beabsichtigte Vorfälle können mit den entsprechenden Monitoring-Tools und EDR-Lösungen frühzeitig erkannt und auch verhindert werden. Die Mitarbeitenden sind das wichtigste Werkzeug im Kampf gegen Cyberbedrohungen. Ein geschulter und sensibilisierter Mitarbeiter kann einen Phishing-Angriff erkennen und richtig reagieren. So wird ein unbeabsichtigter Vorfall zu einer beabsichtigten Abwehr.

Wie erkennt man den Wolf im Schafspelz beziehungsweise im Businesshemd?
Wenn wir hier auch wieder von einem geplanten Angriff oder einem unbeabsichtigten Unfall ausgehen, haben wir verschiedene Möglichkeiten. Ein unachtsamer Benutzer oder eine Mitarbeiterin, die fahrlässig handelt, wird auf Phishing-Kampagnen hereinfallen und auch in den Reports auftauchen, da die Person vermutlich einige Alarme ausgelöst hat. Dort ist es Aufgabe des Unternehmens, proaktiv auf die Person zuzugehen, sie auf ihr Verhalten aufmerksam zu machen und gegebenenfalls in eine Awareness-Schulung zu schicken. Ein geplanter Angriff wird schwieriger zu erkennen sein. Ein Insider stellt eventuell Fragen über Geschäftsprozesse und versucht im Gespräch mit anderen Mitarbeitenden, Informationen einzuholen, die ausserhalb seiner Kompetenz liegen.

Wie können Channelpartner ihre Kunden dabei unterstützen und sie vor Insider Threats schützen?
Das Wichtigste ist, Awareness zu schaffen. Die Technik der IT-Security-Lösungen tut, was sie muss, und sie tut dies auch gut. Das grösste Risiko ist der Mensch. Weitere Möglichkeiten, um es einem Angreifer zu erschweren, ist etwa Zero Trust: Kenne ich wirklich alle Assets in meinem Netzwerk? Dann die Zugriffsrechte regelmässig zu überprüfen. Hat der Mitarbeiter wirklich nur auf das Zugriff, was er für seine tägliche Arbeit benötigt? Monitoring und Alarmierung und der Einsatz von EDR- oder MDR-Lösungen, bei denen eine automatische Remediation durchgeführt wird, sind ebenfalls empfehlenswert. Bei Infinigate bieten wir für unsere Partner und deren Kunden unsere IT-Security-Awareness-Kurse an, um Mitarbeitende auf den neuesten Cybersecurity-Stand zu bringen und somit derartige Risiken zu minimieren.

Alle Interviews finden Sie online
www.it-markt.ch

Michael Unterschweiger
Regional Director ALPS, Trend Micro

Was macht Insider Threats zu einer so grossen Bedrohung?
Michael Unterschweiger: Unternehmen rechnen vor allem mit Cyberbedrohungen von aussen und richten ihre Sicherheitssysteme entsprechend aus. Nach innen sind Analyse- und Erkennungsfähigkeiten hingegen häufig nur eingeschränkt – oder gar nicht – vorhanden. Das führt dazu, dass Insider-Bedrohungen lange unerkannt bleiben und grosse Schäden anrichten können.

Wie gross ist das Risiko für Schweizer Unternehmen?
Das Risiko für Insider-Bedrohungen ist dort besonders hoch, wo grosse Geldbeträge verwaltet oder sensible Informationen wie Zahlungsdaten oder geistiges Eigentum vorhanden sind – also vor allem im Finanzwesen, der Dienstleistungsbranche, dem Detailhandel und dem produzierenden Gewerbe. Gerade diese Branchen machen einen nicht unerheblichen Teil der Schweizer Wirtschaft aus.

Wie unterscheidet man beabsichtigte von unbeabsichtigten Vorfällen? Packt man beide Fälle gleich an?
Gegen böswillige Insider – also beabsichtigte Vorfälle – helfen vor allem ein granulares Rechtemanagement nach dem Least-Access-Prinzip sowie Lösungen wie Data Loss Prevention und Detection & Response. Die unbeabsichtigten Fälle sind noch einmal zu unterscheiden in solche, die wirklich zufällig geschehen – etwa, weil die Mitarbeitenden durch Betrüger überlistet werden – und solchen, bei denen negative Konsequenzen billigend in Kauf genommen werden, weil nachlässige Mitarbeitende vorhandene Policies bewusst ignorieren. Letztere sind besonders schadensträchtig. Während bei Ersteren mit Awareness-Trainings nachgeholfen werden kann, sind bei nachlässigen Insidern vor allem konsequent durchgesetzte Security-Policies notwendig – etwa Update- und Patchmanagement, Credential-Management oder DLP-Regeln.

Wie erkennt man den Wolf im Schafspelz beziehungsweise im Businesshemd?
Bei der Erkennung von nachlässigen Insidern können Angriffs- und Phishing-Simulationen ebenso helfen wie Daten aus einer DLP-Lösung. Geht es um böswillige Insider sind besonders Lösungen für Detection & Response gefragt, um ungewöhnliche Dateizugriffe, Netzwerk-Traffic etc. zu erkennen.

Wie können Channelpartner ihre Kunden dabei unterstützen und sie vor Insider Threats schützen?
Abgesehen vom Ausrollen und der korrekten Konfiguration der genannten Lösungen sind Partner auch als Berater gefragt. Um Bedrohungen von innen und aussen zukünftig wirkungsvoll zu begegnen, werden sich immer mehr Unternehmen für eine Zero-Trust-Strategie entscheiden. Bei deren Planung und Umsetzung benötigen sie Unterstützung.

Cornelia Lehle
Head of Sales DACH, G Data Cyberdefense

Was macht Insider Threats zu einer so grossen Bedrohung?
Cornelia Lehle: Insider Threats sind deutlich schwieriger zu erkennen, denn die Täter kommen aus den eigenen Reihen und müssen weniger Schutzmauern überwinden als Angreifergruppen von aussen. Zahlreiche Schutzmechanismen wie etwa eine Firewall greifen hier einfach nicht. Verdächtige Aktivitäten von Innentätern sind weniger sichtbar, an dieser Stelle braucht es schon ein gutes Monitoring und versierte Angestellte, die solche Aktionen erkennen können.

Wie gross ist das Risiko für Schweizer Unternehmen?
Das Risiko hält sich nicht an Ländergrenzen. Jedes Unternehmen sollte sich der Gefahr bewusst sein, dass es einem Insider Threat zum Opfer fallen kann. Ich halte es für realistisch, dass jährlich jedes zehnte Unternehmen von eigenen Mitarbeitenden betrogen wird – absichtlich oder unabsichtlich.

Wie unterscheidet man beabsichtigte von unbeabsichtigten Vorfällen? Packt man beide Fälle gleich an?
Das ist immer eine Einzelfall-Entscheidung. Bei einem beabsichtigten Vorfall will der Täter oder die Täterin dem Unternehmen aktiv schaden – sei es aus finanziellen Gründen oder aus Rache, etwa wegen einer verweigerten Beförderung. Unbeabsichtigt ist ein Insider Threat, wenn ein Angestellte auf eine Phishing-Mail oder auf Social Engineering hereinfallen und durch die Weitergabe ihrer Credentials Unbefugte ins Netzwerk lassen.

Wie erkennt man den Wolf im Schafspelz beziehungsweise im Businesshemd?
Wenn das so einfach wäre, liesse sich das Problem schnell aus der Welt schaffen. Aber viele Innentäter wissen, wie sie sich unauffällig verhalten müssen. Das ist vergleichbar mit Spionen, die oft jahrelang unerkannt agieren. Letztlich geht es darum, ungewöhnliche Aktivitäten zu erkennen. Betritt eine Person andere Bereiche im Unternehmen, ist sie zu anderen Arbeitszeiten aktiv oder es gibt bei ihrem Benutzerkonto auffällige Aktionen.

Wie können Channelpartner ihre Kunden dabei unterstützen und sie vor Insider Threats schützen?
Der Schutz vor Insider Threats basiert auf den gleichen Prinzipien wie derjenige vor externen Angreifergruppen. Dabei spielen Channelpartner eine wichtige Rolle. Zunächst geht es darum, die gespeicherten Informationen im Unternehmen zu klassifizieren und besonders schützenswerte Daten zu definieren. Dann braucht es eine eindeutige Definition von Nutzerrollen und ein entsprechendes Berechtigungsmanagement. Keine Mitarbeiterin und kein Mitarbeiter muss auf alle Informationen zugreifen können – auch nicht die Vorstände oder Geschäftsführer. Auch eine Netzwerksegmentierung kann den unberechtigten Zugriff auf sensible Informationen verhindern.

Michael Schröder
Manager of Security Business Strategy, Eset Deutschland

Was macht Insider Threats zu einer so grossen Bedrohung?
Michael Schröder: Insider haben bereits Zugang zu den Systemen und in der Regel einen umfassenden Einblick in die internen Prozesse und Daten der Organisation. Da ihre Aktivitäten den normalen Arbeitstätigkeiten ähneln, ist es schwierig, zwischen legitimen und böswilligen Aktivitäten zu unterscheiden. So können vermeintlich kleine (un)beabsichtigte Handlungen, wie die Weitergabe von Kundendaten, Betriebsgeheimnissen oder Sicherheitsvorkehrungen, zu erheblichen Schäden führen. Insider Threats verursachen nicht nur finanzielle Verluste, sondern auch erhebliche Reputations- und Vertrauensschäden.

Wie gross ist das Risiko für Schweizer Unternehmen
Grundsätzlich handelt es sich um eine globale Herausforderung für alle Organisationen. Das Gefährdungspotenzial hängt weniger vom Standort als vielmehr vom eigenen Umgang mit den Risiken ab. Wer eine klare Strategie verfolgt, Zugriffsrechte auf sensible Daten vergibt oder proaktive Massnahmen ergreift, wie etwa Security-Awareness-Programme, Zugangskontrollen, Monitoring und regelmässige Überprüfung der Sicherheitsrichtlinien und -verfahren, ist wahrscheinlich weniger betroffen. Aber auch die beste Strategie nützt nichts, wenn sie nicht gelebt und ständig hinterfragt oder überarbeitet wird.

Wie unterscheidet man beabsichtigte von unbeabsichtigten Vorfällen? Packt man beide Fälle gleich an?
Beide Arten von Vorfällen sollten nicht gleichbehandelt werden. Die Motivation, die Mechanismen und auch die Personengruppen dahinter sind sehr unterschiedlich. Untersuchungen haben gezeigt, dass bis zu 80 Prozent der vorsätzlich herbeigeführten Sicherheitsvorfälle auf betrügerische

Administratoren zurückzuführen sind. Die Abwehr geplanter Vorfälle erfordert robuste Sicherheitsmassnahmen wie Firewalls, Intrusion-Detection-Systeme, Verschlüsselung, Zugangskontrollen und Systeme zur Anomalieerkennung (EDR/MDR). Die Verhinderung unbeabsichtigter Vorfälle erfordert die Schulung und Sensibilisierung des Personals, um menschliche Fehler zu minimieren. Technische Massnahmen wie Datensicherung und die Implementierung von Sicherheitsrichtlinien können ebenfalls dazu beitragen, unbeabsichtigte Vorfälle zu verhindern. Hierzu gehört zum Beispiel auch die Kontrolle externer Medien wie USB-Sticks oder andere Geräte, die einen undokumentierten Datenabfluss erst ermöglichen.

Wie erkennt man den Wolf im Schafspelz beziehungsweise im Businesshemd?
Endpoint Detection & Response (EDR) ist eine wichtige Technologie zur Erkennung und Reaktion auf Insider-Bedrohungen. EDR-Systeme können legitime, aber auch versteckte Prozesse auf Endgeräten überwachen und Muster abnormalen Verhaltens erkennen, selbst wenn der Insider über Zugriffsrechte verfügt. EDR-Systeme erkennen ungewöhnliche Aktivitäten auf Endgeräten, wie das massenhafte Kopieren von Daten, den Zugriff auf ungewöhnliche Dateien oder den Versuch, auf sensible Ressourcen zuzugreifen, die normalerweise nicht benötigt werden. Darüber hinaus kann EDR sensible Daten auf Endpunkten identifizieren und überwachen. Dies ermöglicht die Erkennung von Datenexfiltration durch Insider.

Wie können Channelpartner ihre Kunden dabei unterstützen und sie vor Insider Threats schützen?
Fachhändler bieten ihren Kunden ausser EDR eine Reihe weiterer Möglichkeiten. Es beginnt mit einer umfassende Risikoanalyse, um die spezifischen Bedrohungen und Schwachstellen zu identifizieren. Dies kann auch dazu führen, dass der Fachhändler als Managed Service Provider die Security unterstützt oder komplett übernimmt. Ebenso bieten sich alternative Technologien wie User & Entity Behavior Analytics, Security Information & Event Management und Security Orchestration, Automation & Response an. Auch Cybersecurity-Awareness-Trainings fördern das Bewusstsein für Insider Threats und die Identifizierung verdächtigen Verhaltens. Letztlich ist eine Absicherung nach dem Zero-Trust-Security-Ansatz empfehlenswert.

Gregor Wegberg
Head of Digital Forensics & Incident Response, Oneconsult

Was macht Insider Threats zu einer so grossen Bedrohung?
Gregor Wegberg: Es ist unsere Menschlichkeit. Wir Menschen sind von Natur aus freundlich, hilfsbereit und vertrauensselig – bis wir eines Besseren belehrt werden. Erst recht, wenn es sich um eine Kollegin oder einen Kollegen aus unserem Arbeitsumfeld handelt. Wir können uns kaum vorstellen, dass unser Gegenüber etwas Böses plant oder tun wird. So unterschätzen wir das Risiko, handeln unzureichend und in den meisten Fällen viel zu spät. Sei es, dass wir die Benutzerkonten eines Mitarbeiters nicht sperren, wenn er entlassen wird, oder dass wir den Austausch von sensiblen Dokumenten innerhalb des Unternehmens unzureichend einschränken und überwachen.

Wie gross ist das Risiko für Schweizer Unternehmen?
Niemand weiss es genau. Im Moment liegt der Fokus klar auf Ransomware-Angriffen und damit auf Angriffen aus dem Internet. Diese sind laut, sichtbar und täglich in den Medien präsent. Nur eine Handvoll Unternehmen setzt sich ernsthaft mit dem Risiko von Insiderbedrohungen auseinander. Gleichzeitig sind diese noch weniger bereit, über solche Vorfälle zu sprechen, als es Unternehmen im Zusammenhang mit erlittenen Ransomware-Vorfällen sind. Und auf Basis meiner täglichen Arbeit glaube ich auch, dass diese Priorisierung derzeit die richtige ist.

Wie unterscheidet man beabsichtigte von unbeabsichtigten Vorfällen? Packt man beide Fälle gleich an?
Man sollte immer möglichst unvoreingenommen an ein Ereignis herangehen. Sonst ist die Wahrscheinlichkeit gross, dass man nur Indizien sammelt, die die eigene Meinung bestätigen. Gerade deshalb sind Aussenstehende bei solchen Vorfällen besonders wichtig. Erst nach der Spurensicherung und -auswertung lässt sich eine seriöse Bewertung hinsichtlich Fahrlässigkeit und Vorsatz vornehmen. Eine Unterscheidung findet daher in aller Regel erst im Nachhinein statt.

Wie erkennt man den Wolf im Schafspelz beziehungsweise im Businesshemd?
Dies hängt ganz von der Organisation, den zu schützenden Informationen und dem zugrunde liegenden Bedrohungsmodell ab. Für die meisten Unternehmen ist besondere Vorsicht bei unzufriedenen und ausscheidenden Mitarbeitenden geboten. Eine vertrauens- und respektvolle Unternehmenskultur ist wichtiger, als viele wahrhaben möchten. Unternehmen sollten sich bewusst sein, dass der Schutz vor Insiderbedrohungen ressourcenintensiv ist und eine Vielzahl unterschiedlicher Massnahmen erfordert. Fachexpertise bei der Planung und Umsetzung ist bei dieser Art der Bedrohung sehr zu empfehlen.

Wie können Dienstleister ihre Kunden dabei unterstützen und sie vor Insider Threats schützen?
Vor allem müssen die Kunden über die Grenzen des Angebots informiert werden. Ein Werkzeug allein wird das Risiko nie adäquat adressieren. Im Bereich der Informationssicherheit müssen Werkzeuge immer mit Menschen kombiniert werden, um ihre positive Wirkung entfalten zu können.

Patrick Michel
Principal Consultant, Boll Engineering

Was macht Insider Threats zu einer so grossen Bedrohung?
Patrick Michel: Es ist vor allem die schwierige Kontrollierbarkeit. Das heisst: Mitarbeitende haben per se einen «Pre-Trust» und – abhängig von Funktion und Position – Zugriff auf schützenswerte Daten. Dies öffnet dem Missbrauch Tür und Tor. Es gibt zwar Tools, die dazu beitragen, Insider Threats wie etwa Datendiebstahl zu erschweren. Doch gänzlich verhindern lassen sie sich nicht. Um das Risiko zu minimieren, sind aus meiner Sicht vor allem eine gesunde Firmenkultur, eine faire Entschädigung sowie eine attraktive Tätigkeit notwendig. Glückliche, fair behandelte Mitarbeitende tragen dazu bei, dass kriminelle Machenschaften gar nicht erst in Betracht gezogen werden.

Wie gross ist das Risiko für Schweizer Unternehmen?
Aus meiner Sicht ist das Risiko hierzulande etwas geringer als in anderen Staaten mit einer generell höheren Kriminalität und/oder geringerem Wohlstand. Das Problem darf allerdings auch bei uns nicht unterschätzt werden. Interessant ist dabei die Feststellung, dass in bekannt gewordenen Fällen sehr oft unzufriedene (ehemalige) Mitarbeitende zu Tätern geworden waren. Es lohnt sich folglich, selbst in einer Kündigungsphase fair miteinander umzugehen.

Wie unterscheidet man beabsichtigte von unbeabsichtigten Vorfällen? Packt man beide Fälle gleich an?
Ob ein Vorfall mutwillig oder aus Unvorsichtigkeit geschehen ist, lässt sich im Rahmen detaillierter Untersuchungen eruieren. Lassen sich ein ungewolltes Fehlverhalten – zum Beispiel die Nutzung nicht unterstützter Sharing-Tools oder das Liegenlassen eines Notebooks – im offenen Gespräch sowie durch Sensibilisierungs- und Schulungsmassnahmen adressieren, erfordern vorsätzliche kriminelle Machenschaften eine Anzeige. Dabei nimmt das sogenannte Whistleblowing eine Sonderstellung ein.

Wie erkennt man den Wolf im Schafspelz beziehungsweise im Businesshemd?
Dieser Mitarbeitertypus ist mit einer ausgeprägten kriminellen Energie ausgestattet, wirkt professionell und ist schwierig zu durchschauen. Er ist weder verhaltensauffällig, noch gibt er sich unzufrieden. Folglich lässt er sich primär durch wiederkehrende Kontrollen, etwa Monitoring der Aktivitäten, ausfindig machen.

Wie können Channelpartner ihre Kunden dabei unterstützen und sie vor Insider Threats schützen?
Als wohl wichtigste Massnahme betrachte ich ein weitgefächertes Awareness-Training, gefolgt von der funktions- und positionsgerechten Steuerung der Zugriffsrechte auf Daten sowie technischen Vorkehrungen wie etwa Data-Leak-Prevention-Lösungen und User Behavioral Analytics. Zielführend sind zudem Identity- und Access-Management sowie offensives Security-Testing mit Social-Engineering-Komponenten. Ebenfalls gehören Lösungen zur Überwachung von Internet- und Netzwerkverbindungen sowie zur Erkennung von Anomalien dazu. Grundsätzlich sind Werkzeuge erhältlich, die eine nahtlose Überwachung der einzelnen User ermöglichen. Es ist jedoch immer abzuwägen, wie sich der Einsatz entsprechender Tools auf die Arbeitsmoral der betroffenen Mitarbeitenden auswirkt. Fühlen sie sich überwacht und kontrolliert, schwindet die Motivation. Zudem gilt es, Fragen zum Datenschutz zu klären.

Stefan Rothenbühler
Principal Cyber Security Analyst, Infoguard

Was macht Insider Threats zu einer so grossen Bedrohung?
Stefan Rothenbühler: Mitarbeitende kennen die internen Systeme und Prozesse und verfügen über erforderliche Zugriffsrechte auf Daten. Das erleichtert den unbemerkten Zugriff auf sensible Dokumente oder mögliche Sabotagen. Oft erstreckt sich der Zugriff im Gegensatz zu vielen externen Angriffen über längere Zeit, was die Detektion erschwert. Durch Insider Threats drohen hohe finanzielle und Reputationsschäden.

Wie gross ist das Risiko für Schweizer Unternehmen?
Im internationalen Vergleich sind Schweizer Mitarbeitende tendenziell besser entlohnt und loyaler gegenüber dem Arbeitgeber. Allerdings beheimatet die Schweiz viele multinationale Unternehmen und agiert in sensiblen Geschäftsfeldern wie der Finanzbranche. Andere Motive ausser den finanziellen sind etwa Rache, Neugier oder mangelndes Sicherheitsbewusstsein.

Wie unterscheidet man beabsichtigte von unbeabsichtigten Vorfällen? Packt man beide Fälle gleich an?
Während bei beabsichtigten Vorfällen die Zugriffskontrolle und -überwachung im Vordergrund stehen, können unbeabsichtigte Verstösse vor allem durch Schulungen zur Sensibilisierung der Mitarbeitenden reduziert werden. Bei der Sanktionierung sollte bedacht werden, dass unbeabsichtigte Vorfälle zu absichtlichem Verhalten umschlagen kann, wenn Mitarbeitende darin Vorteile sehen.

Wie erkennt man den Wolf im Schafspelz beziehungsweise im Businesshemd?
Eine offene Kommunikationskultur und ein konstruktiver Umgang mit Fehlern können bei der Erkennung von Insider Threats helfen. Verhaltensänderungen wie vermehrte Geheimhaltung, übertriebenes Engagement oder plötzliche Leistungsschwankungen können Warnsignale sein. Bei gehäuften Auffälligkeiten sollte man gemeinsam mit der Personalabteilung das Gespräch suchen.

Wie können Channelpartner ihre Kunden dabei unterstützen und sie vor Insider Threats schützen?
Externe Partner können bei der Prävention, Detektion und Reaktion Unterstützung bieten. Das umfasst etwa die Unterstützung bei Sensibilisierungsschulungen, Beratungen im Umgang mit Insider Threats oder die Implementierung von Sicherheitslösungen und -konzepten wie Data Loss Prevention, Tools zur Benutzerverhaltensanalyse, Privileged Identity Management und Zero-Trust-Ansätze. Es kann zudem hilfreich sein, diese Vorfälle durch einen externen Partner forensisch aufarbeiten zu lassen – sowohl wegen seiner Unvoreingenommenheit als auch, um gerichtsverwertbare Ermittlungsresultate für arbeitsrechtliche Sanktionierungen zu erhalten.

Marco Eggerling
Chief Information Security Officer EMEA, Check Point Software Technologies

Was macht Insider Threats zu einer so grossen Bedrohung?
Marco Eggerling: Angriffe von innen werden oft von vertrauenswürdigen Mitarbeitenden und Dienstleistern ausgeführt, welche die Schutzmassnahmen kennen und diese zu unterminieren wissen. Daher müssen Sicherheitslösungen kontextbezogen reagieren und Abweichungen von Sicherheits-Baselines erkennen. Diese Form von Risikomanagement ist ein Drahtseilakt, weil Geschäftsprozesse nicht unterbrochen werden sollen, gleichzeitig der Schutz vor unbekannten Akteuren hochgehalten werden muss.

Wie gross ist das Risiko für Schweizer Unternehmen?
Die Gefahrenlage ist in der Schweiz vergleichbar mit anderen Ländern, etwa der EU. Kulturelle Aspekte sind, wenn überhaupt, nur als Nuancen in der Statistik über Insider Threats wahrnehmbar und beeinflussen die Bedrohungslage nicht.

Wie unterscheidet man beabsichtigte von unbeabsichtigten Vorfällen? Packt man beide Fälle gleich an?
Viele Firmen haben sogenannte Joiners-Movers-Leavers-Prozesse. Sobald Mitarbeitende sich verändern, aktivieren sich technische Kontrollen, um schadhaftes Handeln frühzeitig zu erkennen. Jedoch ist ein Generalverdacht der falsche Ansatz. Unbeabsichtigte Vorfälle kommen zumeist in Form von falsch adressierten E-Mails oder falsch platzierten Dokumenten respektive Klassifizierungsänderungen vor. Diese lassen sich mit DLP-Lösungen kontrollieren. Beabsichtigte Vorfälle sind gezielt, geplant und schwer zu prognostizieren. Oft wird mittels benutzerspezifischer Risikoklassifizierung agiert, um Abweichungen zu erkennen – etwa der Upload grosser Mengen von Daten, wenn das bisher nie vorkam.

Wie erkennt man den Wolf im Schafspelz beziehungsweise im Businesshemd?
Mit blossem Auge kaum. User-Entity-Behavior-Analytics-Lösungen können das Benutzerverhalten überwachen und schadhafte Handlungen erkennen. Häufig vollzieht ein Dritter über den Account eines anderen, etwa über ein gehacktes Passwort, Handlungen, die dann schwer zurückzuverfolgen sind. Auch hier kommt das Konzept von benutzerspezifischen Risikoprofilen zum Einsatz. Abweichungen werden erkannt und entsprechend beantwortet. Ein «silver bullet» kann jedoch keine Technologie allein liefern. Vielmehr braucht es hier eine Kombination aus unterschiedlichen Tools.

Wie können Channelpartner ihre Kunden dabei unterstützen und sie vor Insider Threats schützen?
Awareness-Trainings und Sensibilisierung für das Thema sind hier probate Verteidigungsmittel. Wenn jeder wachsam und aufmerksam ist, wird das Risiko für alle automatisch reduziert.