Konzepte für eine IT-Security von morgen

Der Weg zu einer innovativen, transparenten und effektiven Sicherheit

swisscom

Impressum:
© November 2015
Herausgeber/Verlag: Swisscom AG
Autor: Group Security
Redaktion: René Mosbacher, NASKA GmbH
Grafik: Petra Balmer, Bern

Vorwort

Im Bereich der Sicherheit – sei es in der digitalen oder der realen Welt – geht es um die Fragestellung, wie man gewisse wünschenswerte Eigenschaften sicherstellen kann, insbesondere in Anwesenheit eines möglicherweise unsichtbaren Angreifers, der genau diese Eigenschaften zu verhindern versucht. Seit frühester Zeit haben Individuen und Gesellschaften ein Bedürfnis nach Sicherheit. In der realen Welt haben wir über Generationen gelernt, Gefahren zu erkennen und Massnahmen zu deren Abwehr umzusetzen.

Auch im heutigen Umfeld gibt es viele Assets, die wir schützen müssen, um den reibungslosen Ablauf unserer Gesellschaft sicherzustellen. Mit dem ständig wachsenden Einfluss der digitalen Kommunikation und dem Internet of Things auf unsere Gesellschaft setzen wir uns zunehmend neuen Gefahren aus – vor allem weil die Angreifer nun auch aus weiter Ferne ihr Unwesen treiben können.

Glücklicherweise hat die Sicherheitsforschung samt ihrer vielzahligen Anwendungen viele Fortschritte gemacht. Nicht nur die forschungsorientierte Erkenntnis über Sicherheitskonzepte ist gewachsen, sondern auch die anwendungsorientierten Bereiche haben das Thema IT-Sicherheit zu einem profilierten Thema etabliert. Diese Entwicklung ist nicht zuletzt in vielen zum Teil schwerwiegenden Vorfällen für Industrie und Privatanwender begründet. In den letzten Jahren entstand ein fruchtbares Umfeld, um Sicherheitslösungen zu entwickeln und diese in der Praxis anzuwenden.

In diesem Buch werden viele grundlegende Konzepte der IT-Sicherheit anschaulich erläutert. Konkrete Ideen und Modelle, mit deren Hilfe wir die heutige Sicherheit verbessern können, wurden von Swisscom entwickelt und im vorliegenden Buch festgehalten. Ich hoffe, dass Sie viele dieser Konzepte in Ihrem Unternehmen und Ihrem Privatleben umsetzen können.

Ich wünsche Ihnen eine spannende Lektüre.

Prof. Dr. Adrian Perrig,
Network Security Group, ETH Zürich

1 Über diese Publikation

Mit dem Wandel von der Telefongesellschaft zum Anbieter von IT- und Kommunikationslösungen ist die Sicherheit für Swisscom in den letzten Jahren zu einer zentralen Aufgabe geworden. Dem haben wir durch eine akzentuierte Positionierung der Sicherheitsorganisation innerhalb des Unternehmens und durch hohe Investitionen in diesen Bereich Rechnung getragen.

Sicherheit ist zum zentralen Baustein für die Umsetzung des Leitbildes, der Vision und des Kundenversprechens geworden. Dabei geht es uns aber nicht nur darum, sicher, vertrauenswürdig oder zuverlässig zu sein. Vielmehr wollen wir durch einen kreativen Umgang mit dem Thema neue, innovative Lösungen für das Unternehmen finden.

Diese Publikation soll Interessierten einerseits einen gerafften Überblick über den generellen Stand und die Konzepte der IT-Sicherheit vermitteln. Andererseits soll sie zeigen, wie wir das Thema angehen und welche Erfahrungen wir dabei gemacht haben. Ein Teil der beschriebenen Konzepte und Massnahmen sind generisch und können auch in anderen Unternehmen umgesetzt werden. Zudem zeigen wir in Fallstudien, welche Überlegungen zu welchen Lösungsansätzen geführt und wie sie sich bewährt haben.

Zur Begriffswahl
Der Einfachheit halber fassen wir alle Organisationen, für die IT-Sicherheit relevant sein könnte, unter dem Begriff «Unternehmen» zusammen. Das operative Gebiet der Sicherheit nennen wir «Sicherheit» (gelegentlich «Security»), und die organisatorische Einheit, die für die Sicherheit zuständig ist, heisst im Folgenden «Sicherheitsorganisation».

2 Trends in der Wirtschaft

Während der letzten fünf, zehn Jahre hat die Wirtschaft verschiedene Trends erlebt, die die Sicherheit der ICT beeinflussen. So war es beispielsweise vor dem Erscheinen der ersten Smartphones klar, dass die IT – und nur sie – die notwendigen Mittel für die Arbeit mit Daten zur Verfügung stellt. Klar war auch, dass mit dem Verlassen des Büros der Zugang zu den Firmendaten gekappt wird. Dies hat sich mittlerweile dramatisch geändert.

2.1 Consumerization of IT

Angefangen hat es mit dem Wunsch der Geschäftsleitung, auch von ausserhalb auf die Geschäftsinfrastruktur zugreifen zu können. Das brachte manche IT zwar in eine verzwickte Lage – aber wer mag schon dagegenhalten, wenn dies der Wunsch des obersten Führungsgremiums ist? Damit war die «Consumerization of IT» geboren, ein Trend, den wir heute unter Bring your own Device (BYOD) kennen.

Das Bedürfnis, mit dem privaten Gerät im Firmennetz zu arbeiten, wanderte bald entlang der Hierarchien nach unten. Dies haben sich mittlerweile verschiedene Firmen zur Tugend gemacht, indem sie ihren Mitarbeitenden generell erlauben, eigene Geräte ins Büro mitzubringen. Im Extremfall gilt das nicht nur für Smartphones, sondern für die ganze Palette an prozessorbewehrten, netzfähigen Geräten, bis hin zum Notebook.

Spinnt man das Konzept weiter, dann wird es in Zukunft Firmen geben, die ihren Mitarbeitenden nur noch ein Budget statt der IT-Ausrüstung bereitstellen. Dem stehen heute zwar noch rechtliche Hürden im Weg: Es gilt beispielsweise, die Aufteilung von Investitions- und Betriebskosten zwischen den Parteien zu regeln. Auch für den Fall von Verlust oder Reparatur müssen im Voraus Lösungen gefunden werden. Vom Trend her ist aber absehbar, dass BYOD den Nutzer je länger je mehr zum CIO macht. Damit definiert er die IT-Strategie seines Unternehmens mit. Dies wird natürlich auch die IT-Sicherheit stark beeinflussen – doch dazu später mehr.

Bei Swisscom ist der Einsatz privater Geräte seit einiger Zeit offiziell zugelassen und wird auch gefördert. Die Strategie des Any Device wurde vom Verwaltungsrat verabschiedet – somit hat jeder Mitarbeitende die Möglichkeit, entweder ein offizielles Gerät zu beziehen oder sein eigenes zu verwenden.

Basierend auf diesen Entscheiden hat auch die IT-Infrastruktur begonnen, sich danach auszurichten. Da den Any Devices aus Gründen der Sicherheit der Zugang zum internen Firmennetz verwehrt bleibt, werden die notwendigen Dienste via Internet zur Verfügung gestellt. Das stellt aber wiederum zusätzliche Anforderungen an die Sicherheit – beispielweise bei der Authentisierung oder der Verschlüsselung.

2.2 Big Data

Dass bei verschiedenen Geschäftsprozessen eine Menge Daten anfallen, ist nicht neu. Neu sind auch nicht die Überlegungen zu den Geschäftsmodellen, die darauf beruhen. Hinzugekommen ist allerdings die Möglichkeit, diese enormen Datenmengen auch effektiv und effizient zu verarbeiten.

Die Verwendung von Big-Data-Analysen wirft in erster Linie Fragen zum Datenschutz auf. Im Prinzip gelten hier dieselben Regeln wie bei «normalen» Datenbanken, und auch das Konzept des Anonymisierens ist eigentlich nicht neu. Das wirkliche Problem – das bereits seit den Anfangszeiten der Data Warehouses besteht – ist die Datenkorrelation. Studien haben gezeigt, dass – speziell wenn Bewegungsdaten involviert sind – maximal vier Datenpunkte reichen, um ziemlich eindeutig auf eine Person rückschliessen zu können. Es gibt zwar bereits gute Ansätze, die eine wirkliche Anonymisierung der Daten erlauben. Wichtig sind aber eine klare Governance und die strikte Kontrolle, um sicherzustellen, dass kein Missbrauch betrieben wird. Wir haben es hier also, wie so oft, nicht mit einer technischen, sondern einer prozeduralen und letztlich einer ethischen Aufgabe zu tun. Ein mass- und verantwortungsvoller Umgang ist deshalb bei Big Data essenziell.

2.3 Internet of Things

Je länger je mehr verbinden sich nicht nur Menschen über das Internet, sondern auch Maschinen. Dies ist per se nicht neu. Die Industrie automatisiert und verknüpft ihre Systeme schon seit Jahrzehnten und hat dabei die sogenannte Maschine-zu-Maschine-Kommunikation eingeführt. Leider werden vernetzte Geräte vor allem entwickelt, um möglichst effizient zu arbeiten – die (Daten-)Sicherheit hat dabei oft nur einen untergeordneten Stellenwert.

Auch während ihres Betriebs werden vernetzte Geräte eher als Teil des Gebäudes behandelt und nicht zwingend als Teil eines grösseren Netzes. Deshalb ist es nicht erstaunlich, dass solche Geräte im Internet oft gänzlich ohne Authentisierung oder unter Standard-Benutzernamen und -Passwort steuerbar sind. Damit kann, wer will, zum Beispiel die Klimaanlage leicht von «aussen» kapern und nach Belieben manipulieren. In Räumen, in denen die Temperatur wichtig ist (etwa in Rechenzentren), ist das natürlich eine fatale Schwachstelle.

Weiter läuft auf den meisten solchen Geräten kommerzielle Software, die regelmässige Wartung benötigt. Bei IT-Systemen ist dies Stand der Technik – bei Produktionsanlagen hingegen ist Patch Management vielerorts ein Fremdwort geblieben. Schlimmer noch: Einige Hersteller von Industrieanlagen unterbinden die Wartung der Systemsoftware durch den Betreiber, indem sie mit Garantieverlust drohen. Das Resultat sind dann wiederum Sicherheitslücken, die relativ einfach ausgenützt werden können.

Ähnliche Probleme entstehen, wenn sich die Lebenszyklen mechanischer und elektronischer Komponenten stark unterscheiden. Industriemaschinen werden häufig für den Einsatz über zehn bis 20 Jahre konzipiert, aber auf der Basis von Standardsoftware entwickelt. Dummerweise liegt die Lebenserwartung solcher Software bei nur zehn Jahren. Danach liefern die Hersteller kaum Sicherheits-Patches mehr.

Aber dies ist erst der Anfang der Entwicklung. Im Zusammenhang mit der Energiewende kommt jetzt auch der Wunsch nach mehr Hausautomation auf. Die Idee dahinter: Automatisierte Gebäudetechnik soll den Energieverbrauch senken. Das ist eine hervorragende Idee, sofern die Sicherheit von Beginn an mit eingeplant wird. Wenn nicht, laufen wir Gefahr, dass unsere Heizung oder die Stromversorgung von aussen manipuliert werden kann – entweder aus bösem Willen oder aus Unachtsamkeit.

2.4 Dezentrale Entwicklung

In den meisten Firmen war und ist die Governance der Software-Entwicklung noch zentralisiert. Das bedeutet: Der Prozess, mit dem das Business von der Idee zur Lösung kommt, ist strikt vorgegeben und eng geführt. Dies erleichtert einer Sicherheitsorganisation (und vielen anderen zentralen Diensten) das Leben insofern, als sie früher oder später sowieso ins Projekt involviert wird. Unter solchen Voraussetzungen reicht es, den Standard-Entwicklungsprozess zu unterstützen und somit auf die notwendigen Sicherheitsmassnahmen einzuwirken.

Neuerdings gehen Firmen aber vermehrt zur dezentralen Entwicklung über. Das erlaubt ihnen, mit kleinen, effizienten Teams näher am Business zu entwickeln. Das geht schneller und hat den Vorteil, im ungünstigsten Fall schnell und zu tieferen Kosten zu scheitern.So unterstützenswert dieser Trend ist – er stellt die Governance vor völlig neue Herausforderungen. Unter solchen Rahmenbedingungen muss die Linie viel mehr Verantwortung übernehmen. Hierfür braucht sie aber Hilfe von der Sicherheitsorganisation. Sie muss Antworten darauf geben, wie Firmenrisiken in solchen Umgebungen noch sinnvoll gemanagt werden können. Mehr dazu in Kapitel 7.2.

Die dezentrale oder verteilte Entwicklung wird bei Swisscom aktiv gefördert. Dies schafft für die Beteiligten neue Voraussetzungen: Auf der einen Seite müssen die Geschäftsbereiche eine Verantwortung übernehmen, die sie in der zentralisierten Struktur nie hatten. Sie sind neu nicht nur verantwortlich für die inhaltliche Umsetzung, sondern auch für die Qualität und die Sicherheit. Bei Swisscom wird vieles auf der technischen Seite durch klar definierte Schnittstellen (APIs) geregelt.

Aus dem Blickwinkel der Sicherheit heisst das: Es muss jederzeit klar sein, wer der Risiko-Owner ist, und die Sicherheitsorganisation muss eine enge Bindung ans Business haben. Weiteres zu den organisatorischen Aspekten liefert Kapitel 7.4.

2.5 Globalisierung versus Rückkehr zu autarken Diensten

Der Trend zum globalen Sourcing war und ist unverkennbar. Begonnen hat es mit dem Outsourcing der Entwicklung nach Indien, später nach Osteuropa. Einen vorläufigen Höhepunkt hat dieser Trend mit der Verlagerung in die Cloud erreicht. Das Ziel dabei war klar die Reduktion der Kosten.

Wohin die Reise am Ende noch führen wird ist hingegen nicht so klar. Die Industrie bewegt sich hier auf einem schmalen Grat zwischen Kostensenkung und den Sicherheitsanforderungen. Dabei verunsichert die unklare internationale Rechtssituation (Stichwort Patriot Act). Und die Enthüllungen rund um die Aktivitäten der Nachrichtendienste hinterlassen bei vielen ein zunehmend mulmiges Gefühl beim Gedanken, Daten oder Dienste ins Ausland zu verschieben. Da darf es nicht erstaunen, wenn verschiedene Staaten dazu tendieren, ihre Regulatorien wieder mehr in Richtung lokale Datenhaltung auszurichten. Diese Entwicklungen sind sicher noch nicht abgeschlossen.

3 Trends im Privaten

3.1 Always on, Sensoren überall

Was den privaten Bereich angeht hat sich in den letzten Jahren eine permanente Online-Verbindung mit dem Netz breit durchgesetzt. Wir haben uns daran gewöhnt, die Informationen, die wir benötigen, jederzeit zur Verfügung zu haben. Das ist sicher eine spannende Entwicklung, die viele Möglichkeiten eröffnet. Gleichzeitig ist sie aber auch bedenklich, wenn wir uns klar werden, welche Datenspuren wir im Netz hinterlassen und welchen Einfluss dies auf unsere Privatsphäre hat. Die Frage ist auch, welche Prozesse noch funktionieren, sollte dieses «Always on» einmal wegfallen.

Unser Leben wird zunehmend von einer Armada an Sensoren vermessen. Am offensichtlichsten ist dies bei all den Geräten, die aus medizinischen Gründen bestimmte Körperfunktionen kranker oder älterer Menschen erfassen und übermitteln. Solche Sensoren können eine grosse Hilfe sein, etwa indem sie älteren Menschen ermöglichen, länger in ihrer gewohnten Umgebung zu leben. Wenn der Gesundheitszustand zu Hause überwacht wird, kann beispielsweise automatisch ein Alarm ausgelöst oder ein Arzt aufgeboten werden, sollte eine Körperfunktion einen kritischen Wert erreichen.

Den meisten Nutzern von Fitness-Apps dürfte klar sein, dass ihr Aktivitätsstatus und ihr Standort erfasst und an einen Server irgendwo in der Welt übermittelt werden. Dass aber auch viele andere, auf den ersten Blick unverdächtige Apps, laufend Daten über uns und unser Verhalten sammeln, ist vielen eher unbekannt.

Dies wirft natürlich unmittelbar Fragen zum Datenschutz und zur Wahrung unserer Privatsphäre auf. Weiter sollten wir uns auch fragen, wie weit solche Systeme – durch personalisierte Werbung etwa oder Tipps – unser Verhalten beeinflussen oder gar manipulieren können.

4 Die Bedrohungslage

Um die Entwicklung der Bedrohungslage zu verstehen, sollten wir zuerst einmal die Hintergründe beleuchten. Grundsätzlich hat sich die Rolle des Internets in den letzten Jahren stark verändert. Was den Sicherheitsaspekt betrifft: Ursprünglich wurde das Netz von Hackern häufig genutzt, um Software und «Toolkits» zu vertreiben. Mit solchen Programmen lassen sich auf Rechnern bekannte Schwachstellen ausnutzen. Da die Hackerwerkzeuge vorgefertigte Schadfunktionen bereitstellen, ermöglichen sie es Angreifern, Systeme zu kompromittieren, auch wenn sie über kein vertieftes technisches Wissen verfügen. Mit solchen Werkzeugen kann also fast jede und jeder Angriffe starten.

Diese entsprechenden Werkzeuge wurden und werden über einschlägige Websites, oft via Darknet vertrieben. In den letzten Jahren hat sich dort ein wahrer Untergrundmarkt gebildet. Mittlerweile werden neben Angriffssoftware auch Dienstleistungen wie das gezielte Angreifen von bestimmten Systemen oder Organisationen angeboten. Wer will, kann auch Aufträge für das Versenden von Spam-Mails vergeben und vieles mehr. Dieser Untergrundmarkt steht im Prinzip jedem offen, der einen vernetzten Rechner, kriminelle Energie und das nötige Kleingeld hat.

4.1 Akteure

Die Angreifer lassen sich in verschiedene Gruppen unterteilen. Zuerst wird unterschieden zwischen solchen, die opportunistisch, und solchen, die gezielt vorgehen. Bei eher opportunistischen Akteuren wie den Script Kiddies kann davon ausgegangen werden, dass sie sich die schwächsten Opfer suchen. Gegen solche Akteure hilft es oft schon, schlicht «besser» als andere Unternehmen zu sein. Dann wird in den meisten Fällen das Geschäftsmodell der Angreifer nicht aufgehen. Mit anderen Worten: Die Kosten für einen Angriff müssen entsprechend hoch sein. Ein funktionierender Grundschutz kann hier durchaus helfen.

Anders verhält es sich mit Akteuren, die gezielt vorgehen. Sie wollen ein bestimmtes Ziel erreichen und werden dies mit aller Konsequenz und allenfalls unter Einsatz von grossen personellen und finanziellen Mitteln verfolgen. Sich gegen solche Akteure zu schützen, ist deutlich schwieriger und teurer. Betrachten wir verschiedene Vertreter dieser Spezies näher.

*Bild 1: **Die Angreifer und ihre Vorgehensweise. Der Aufwand und die Kosten für den Schutz gegen ihre Aktivitäten steigen von unten nach oben.***

4.1.1 Vandalen

Digitale Vandalen verfügen häufig über kein sehr fundiertes Wissen. Sie verstehen Angriffe auf eine Infrastruktur eher als sportliche Herausforderung und benutzen hierfür üblicherweise Software und Anleitungen, die sie im Internet finden können. Sie nutzen die Schadsoftware, ohne zu verstehen, wie sie im Detail wirklich funktioniert.

In den Anfängen des Internets gehörte Vandalismus – vor allem durch Jugendliche – zu den grössten Bedrohungen. Die grundlegenden Schutzmechanismen waren damals noch nicht vorhanden oder ausgerollt. Heute sollten Vandalen eigentlich kein grosses Problem mehr sein. An einer gut gewarteten Infrastruktur dürften ihre Angriffe sehr wahrscheinlich abprallen – ganz vernachlässigen lassen sich die Risiken durch Vandalen indessen nicht.

Die Kernfrage im Zusammenhang mit den Vandalen ist, welche Werkzeuge ihnen in Zukunft zur Verfügung stehen werden. Werden sie im Netz schon bald Hilfsmittel finden, die heute noch den professionellen Angreifern vorbehalten sind? Falls ja, könnten sie wieder sehr viel gefährlicher werden.

4.1.2 (Organisierte) Kriminalität

Die Kriminalität bewegt sich immer mit dem Geld. Deshalb ist es logisch, dass mit der fortschreitenden Kommerzialisierung des Internets auch die Kriminellen dort auftauchen. Egal, ob es um Betrügereien oder um Datendiebstahl geht – solange sich damit Geld verdienen lässt, werden Kriminelle dort ihr Unwesen treiben.

Technisch und konzeptionell haben sich die Kriminellen in den letzten Jahren massiv weiterentwickelt. Während sie früher als Einzeltäter auftraten, stehen wir heute vermehrt lose verbundenen Banden gegenüber. Sie finden sich auf Untergrundmärkten und spannen für Projekte zusammen. Eine wichtige Währung in diesem Umfeld ist der Ruf, den ein Krimineller in der Szene hat. Die Banden suchen sich Mitglieder mit geeignetem Profil. Gefragt sind ebenso technische Fähigkeiten wie Hehlerdienste, über die sich gestohlene Daten oder Kreditkartennummern verkaufen lassen. Wirklich hierarchisch organisierte verbrecherische Organisationen agieren indes bis heute eher selten in der virtuellen Welt.

Auch die Cyberkriminellen sind in den letzten Jahren deutlich professioneller geworden. Ein Grund dafür sind die gesunkenen Kosten und die breitere Verfügbarkeit leistungsfähiger IT. Vor diesem Hintergrund muss es das Ziel sein, die Kosten der Kriminellen so weit hochzutreiben, dass sich ihr «Business Case» nicht mehr rechnet. Hierfür muss man aber dauernd am Ball bleiben, weil auch die Kriminellen laufend technisch aufrüsten und ihre Angriffsmethodiken verbessern.

4.1.3 Hacktivists

Eine neuere Erscheinung sind die Hacktivists. Gruppierungen wie Lulsec und Anonymous haben in den letzten Jahren mit spektakulären Aktionen gezeigt, dass sie eine ernstzunehmende Bedrohung sein können. Sie sind in der Lage, hochkompetente Leute zu gewinnen, denen es immer wieder gelingt, ganze Infrastrukturen lahmzulegen oder zumindest in ernsthafte Schwierigkeiten zu bringen. Dabei geht es ihnen vor allem darum, politische oder ideologische Zeichen zu setzen.

Wir müssen grundsätzlich davon ausgehen, dass die Leute, die hier gratis mitarbeiten, mindestens teilweise dieselben sind, die auf den erwähnten Untergrundmärkten ihre Dienste für Geld anbieten. Die Hacktivists selbst haben indessen weder die finanziellen Mittel noch das Bedürfnis, Dienstleitungen im Untergrund einzukaufen.

4.1.4 Terroristen

Hinsichtlich Terrorismus ist die Industrie geteilter Meinung: Die einen glauben, dass Terroristen kein Interesse haben, ICT-Infrastrukturen anzugreifen, da sie das Internet als Kommunikationsmedium und Rekrutierungskanal benutzen. Andere weisen darauf hin, dass sich der westlichen Welt gerade durch gezielte Angriffe auf die ICT-Infrastruktur grössere Schäden zufügen lassen als mit anderen Mitteln. Dem steht wiederum entgegen, dass heutige Terroristen auf möglichst grosse Medienwirksamkeit aus sind. Angriffe auf die ICT sind aber bei weitem nicht so medienwirksam wie etwa Attentate auf Leib und Leben. Kommt hinzu, dass sich die Nachricht über einen Angriff auf die kritische ICT-Infrastruktur unter Umständen überhaupt nicht mehr verbreiten lässt, weil die Kommunikationskanäle nicht mehr funktionieren.

Bis vor kurzem ging man davon aus, Terroristen fehle das Know-how für einen erfolgreichen Angriff auf die ICT-Infrastruktur, und sie könnten es auch nicht kurzfristig aufbauen. Dies ist aber gar nicht mehr nötig, weil sie das erforderliche Wissen mit genügend Geld einfach kaufen können. Zudem haben verschiedene Regierungen begonnen, militärische Cyber-Einheiten zu schaffen, die auch Angriffe führen können. Sollten dort dereinst Stellen abgebaut werden, kommen plötzlich gut ausgebildete Fachleute auf den Markt, die ihr Wissen unter Umständen im Untergrund anbieten.

4.1.5 Geheimdienste

In den letzten Jahren haben gezielte Angriffe durch Geheimdienste massiv zugenommen. Auch wenn die Berichterstattung oft ein anderes Bild vermittelt, gilt es klarzustellen, dass solche Angriffe aus allen Teilen dieser Welt kommen. Ob Geheimdienste aggressiv agieren, hängt davon ab, wie sie in ihren Ländern organisiert sind. Je nach gesetzlicher Grundlage sollen sie nur den Staat schützen oder eben zusätzlich auch die heimische Wirtschaft unterstützten – sprich Industriespionage betreiben.

Regierungen, die ihre Nachrichtendienste für die Industriespionage einsetzen, sind heute ein sehr ernst zu nehmendes Problem. Ihre Spionage-Organisationen haben die Mittel und die Möglichkeiten, Angriffe von langer Hand mit hochqualifiziertem Personal zu planen und durchzuführen. Zudem sind sie in der Lage, ICT-Produkte quasi ab Fabrik zu kompromittieren. Dann kauft die IT des Unternehmens Schwachstellen und Hintertüren bereits mit den Geräten zusammen ein, ohne dass sie es ahnt.

Ein derart kompromittiertes Netz kann dann für Spionage und Sabotage genutzt werden. Und weil verschiedene Staaten offensive Organisationen für den «Cyber-Krieg» aufbauen, müssen wir davon ausgehen, dass sie diese Möglichkeiten im Zweifelsfall auch nutzen werden. Dies sind momentan zwar nur Vermutungen, aber wir müssen solche Szenarien im Auge behalten und davon ausgehen, dass die Bedrohung weiter steigt.

4.2 Was kommt noch auf uns zu?

Zur Beurteilung der Bedrohungslage müssen neben den Akteuren auch die Trends bei den Bedrohungen betrachtet werden. Eine gutes Hilfsmittel hierfür sind sogenannte Bedrohungsradare, wie sie ähnlich von staatlichen Sicherheitsdiensten für die Lagebeurteilung entwickelt wurden. Wie ein Bedrohungsradar im Einzelnen aufgebaut und zu verstehen ist, kann im Anhang nachgelesen werden. Im Folgenden beleuchten wir nur kurz die grossen, momentan zu beobachtenden Trends.

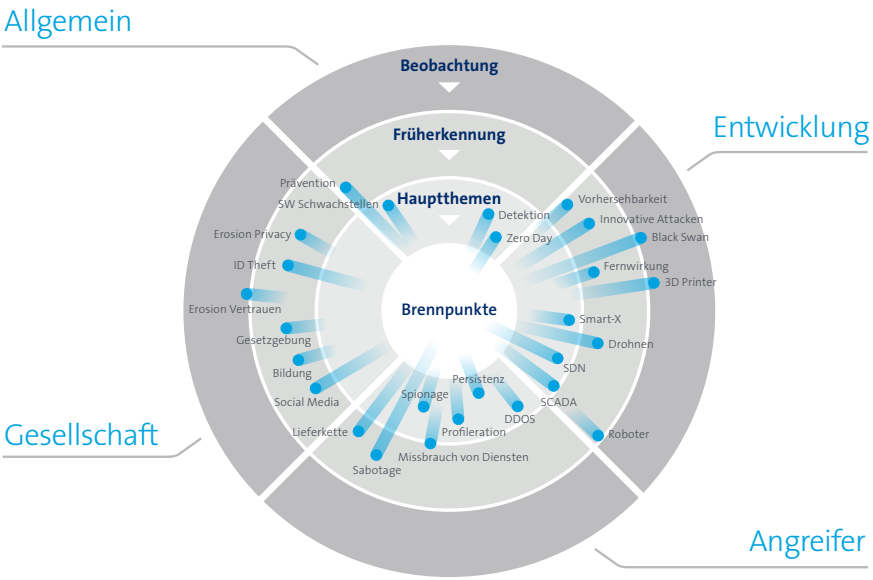


Bild 2: Das Bedrohungsradar gibt Auskunft über die Entwicklung der unterschiedlichen Bedrohungsarten und -kanäle.

4.3 Fazit

Kriminalität: Wir rechnen nicht damit, dass die Menge an kriminell motivierten Angriffen in den nächsten Jahren substanziell zunimmt. Wie schon erwähnt werden kriminelle Kräfte zudem Zugang zu Werkzeugen und Angriffstechniken erhalten, die bisher nur gut ausgebildeten Organisationen mit entsprechendem Budget zur Verfügung standen. Als Folge davon werden wir uns auch auf komplexere Angriffe einstellen müssen. Zudem lässt sich feststellen, dass sich kriminelle Organisationen mehr Zeit für einen Angriff nehmen, dafür dann aber grösseren Schaden anrichten. Die Angriffe werden professioneller.

Gezielte Angriffe: Wir müssen davon ausgehen, dass gezielte Angriffe weiter zunehmen. Dazu gehören solche, die zum Ziel haben, einer bestimmten Organisation zu schaden. Weiter ist zu erwarten, dass solche Angriffe überraschender werden und Methoden kombinieren, die sich bisher nicht kombinieren liessen. Gezielte Angriffe werden also künftig unvorhersehbarer.

Internet of Things: Das Internet of Things bietet ein gigantisches Potenzial für die Automatisierung – aber auch für Angriffe. Die Verwundbarkeit breit eingesetzter Software-Bibliotheken wirkt sich nun plötzlich nicht «nur» auf klassische Computer aus, sondern auf «Things» wie Autos, Kühlschränke oder Fernseher. Nur in seltenen Fällen setzen sich die Hersteller solcher Produkte mit dem Lebenszyklus der Gerätesoftware auseinander. Entsprechend sind sie dann auch nicht in der Lage, kurzfristig auf kritische Schwachstellen zu reagieren. Wenn solche Schwachstellen in verschiedenen Komponenten vorkommen, wird das Schadenspotenzial enorm.

5 Sicherheitsgrundsätze

Anhand des bisher Gesagten lassen sich vier Grundsätze ableiten, die als Basis für jede Sicherheitsstrategie gelten sollten.

5.1 Die Security Good Practice muss umgesetzt sein

Grundlage für jegliche neuen und bahnbrechenden Ideen hinsichtlich Sicherheit bildet eine solide und stabile operationelle und konzeptuelle Basis. Hierfür gilt es, eine klassische Security Good Practice zu implementieren und am Leben zu erhalten. Dazu gehört eine breite Palette von Anforderungen wie:

- Ein stabiles und gelebtes Policy Framework mit entsprechender Security Governance
- Ein stabiles und pragmatisches Risiko-Management
- Eine Organisation, die sich integrierte Sicherheit als Ziel setzt
- Operationelle Prozesse wie Patch Management, Identity Management, Incident Management
- Training, Awareness und Kommunikation
- Secure Software Development

Je nach Infrastruktur und Organisation können noch weitere Anforderungen hinzukommen.

Die üblichen Security Frameworks decken diese Themen in ihrer ganzen Breite ab. Mit ISO 27001 lassen sich diese Aufgaben auch durch externe Firmen zertifizieren. Dabei gilt es aber zu berücksichtigen, dass diese Norm höchstens als erster Schritt hin zu einer stabilen Basis verstanden werden darf. Sicherheit ist ja ein kontinuierlicher Prozess.

5.2 Sicherheit ist der nächste Business-Treiber

Sicherheitsorganisationen sind entstanden, um die Werte eines Unternehmens zu schützen. Dies ist unbestrittenermassen nach wie vor eine ihrer wichtigsten Aufgaben – aber eben nicht die einzige. Zu lange haben sich Sicherheitsorganisationen auf der Grundhaltung ausgeruht, dass Sicherheit notwendig und Compliance das höchste Gut sei. Dabei haben sie aber übersehen, dass die hierfür erforderlichen Massnahmen und Konzepte für viele Führungskräfte eher ein notwendiges Übel waren und oft noch sind.

Zu häufig spielen die Sicherheitsorganisationen noch auf der Klaviatur der Katastrophenszenarien. Sie argumentieren: Wenn man nicht genügend investiert, werden üble Dinge geschehen. Auch wenn dies durchaus den Tatsachen entspricht, wird kaum ein Budget-Verantwortlicher frohen Herzens die nötigen Gelder sprechen.

Wer aus diesem Standpunkt heraus agiert, vergisst, dass der Begriff ICT-Sicherheit durchaus positiv aufgeladen werden kann. Was es braucht, ist die richtige Dosis an positiven Botschaften. So liesse sich etwa darauf hinweisen, dass die passende IT-Sicherheit erst die Voraussetzungen für Home Office und BYOD schafft. Oder es könnte gegenüber der Geschäftsleitung argumentiert werden, dass dank der Sicherheit die Risiken strategischer Entscheidungen plötzlich transparent werden. Damit wird die Sicherheit zum Enabler – und der Chief Security Officer zum Partner.

Hierfür braucht es aber neue Denkansätze seitens der Sicherheitsfachleute. Vor allem müssen sie sich weg von der extrinsischen hin zur intrinsischen Sicherheit bewegen. Bei ersterer wird versucht, um unsichere Produkte eine Sicherheit herumzubauen. Bei zweiterer werden Produkte von vornherein sicher gebaut. In extrem verteilten Systemen wie etwa dem Internet der Dinge ist der zweite Ansatz eindeutig der praktikablere, um Sicherheit zu gewährleisten.

Wir haben gelernt, dass die Business- und Budget-Verantwortlichen bei Weitem nicht abgeneigt sind, Geld für Sicherheit auszugeben. Sie tun dies aber nicht, weil es die Sicherheitsorganisation so anordnet, sondern weil sie verstehen, dass es nötig ist, um die gesteckten Ziele zu erreichen. Dabei ist es zentral, dass die Sicherheitsorganisation als Partner agiert, aber gleichzeitig auch zeigt, warum sie so denkt, wie sie denkt. Ein gemeinsames Verständnis für die Bedrohungslage ist dabei ein wichtiger Ausgangspunkt.

5.3 Wir werden laufend angegriffen

Es ist eine Binsenwahrheit, dass Netze heute laufend angegriffen werden. Neu ist die Qualität der Angriffe. Früher ging man noch davon aus, das Firmennetz und die Firmenrechner seien sauber und vertrauenswürdig. Heute müssen wir aber annehmen, dass kriminelle Elemente oder Drittstaaten bereits die Lieferkette kompromittieren. Weiter wäre es vermessen, bei der Menge und Komplexität der Angriffe davon auszugehen, alle würden erfolgreich abgewehrt werden können. Deshalb empfiehlt es sich eine Architektur so zu bauen, als sei das interne Netz bereits kompromittiert.

5.4 Intelligence ist die Basis der Detektion

Wer die Grenzen der Prävention akzeptiert, weiss, wie wichtig es ist, die Detektion und Intervention entsprechend zu stärken. Das Ziel soll sein, dass diese beiden Bereiche für Aussenstehende unvorhersehbar agieren. Ein Angreifer darf nicht wissen was ihn erwartet. Deshalb müssen speziell bei der Datensammlung für die Intelligence und auch bei der Detektion neue Wege beschritten werden.

Aber damit noch nicht genug: Offensichtlich reicht es nicht, wenn Angriffe detektiert werden – das Unternehmen muss auch in der Lage sein, darauf zu reagieren. Dies wirkt sich wiederum auf die Technik aus (einige Ideen hierzu werden im Kapitel 8.2 beschrieben). Und selbstverständlich hat das auch Konsequenzen für die Prozesse und die Zusammenarbeit der Unternehmensbereiche (mehr hierzu im Kapitel 8.3).

6 Aktionsfelder der Sicherheitsorganisation

Die Einflussmöglichkeiten einer Sicherheitsorganisation erstrecken sich über die Bereiche Grundlagen, Prävention, Detektion und Intervention. Im Folgenden gehen wir auf jeden Bereich ein und zeigen, was dort im Normalfall sinnvoll und möglich ist. Dabei erheben wir keinen Anspruch auf Vollständigkeit – je nach Infrastruktur und Unternehmen können weitere Punkte dazukommen oder allenfalls auch wegfallen.

Bild 3: ***Die vier Einflussbereiche der Sicherheitsorganisation.***

6.1 Grundlagen

Unter Grundlagen verstehen wir das Fundament, auf dem die weiteren Bereiche aufbauen. Damit wird klar, dass die Grundlagen stabil und zuverlässig funktionieren müssen. Dies betrifft hauptsächlich die Grundschutz-Vorgaben, die Prozesse und die Technik, die eine «Security Good Practice» bilden.

6.2 Prävention

Der Nutzen der Prävention ist recht offensichtlich, denn da fühlt sich die Sicherheitsorganisation ursprünglich zu Hause. Hier gilt es je nach Voraussetzungen, Massnahmen bei den Mitarbeitenden, der Technik und den Prozessen zu ergreifen. Typische Beispiele aus diesem Umfeld sind:

- Training und Verbesserung der Awareness: Was müssen die Mitarbeitenden wissen respektive können?
- Continuity Management: Wie kann sichergestellt werden, dass das Business auch bei Verlust der IT noch funktioniert?
- Resilience (Ausfallsicherheit): Hier geht es darum, sicherzustellen, dass die Systeme auch dann weiter funktionieren, wenn eine Komponente ausfällt oder kompromittiert wurde.
- Security Risk Management: wird oft mit dem Risiko-Reporting verwechselt. Das Ziel ist nicht (nur), die Risiken zu kennen, sondern auch aktiv zu managen.
- Weiteres, je nach Organisation und Infrastruktur.

6.3 Detektion

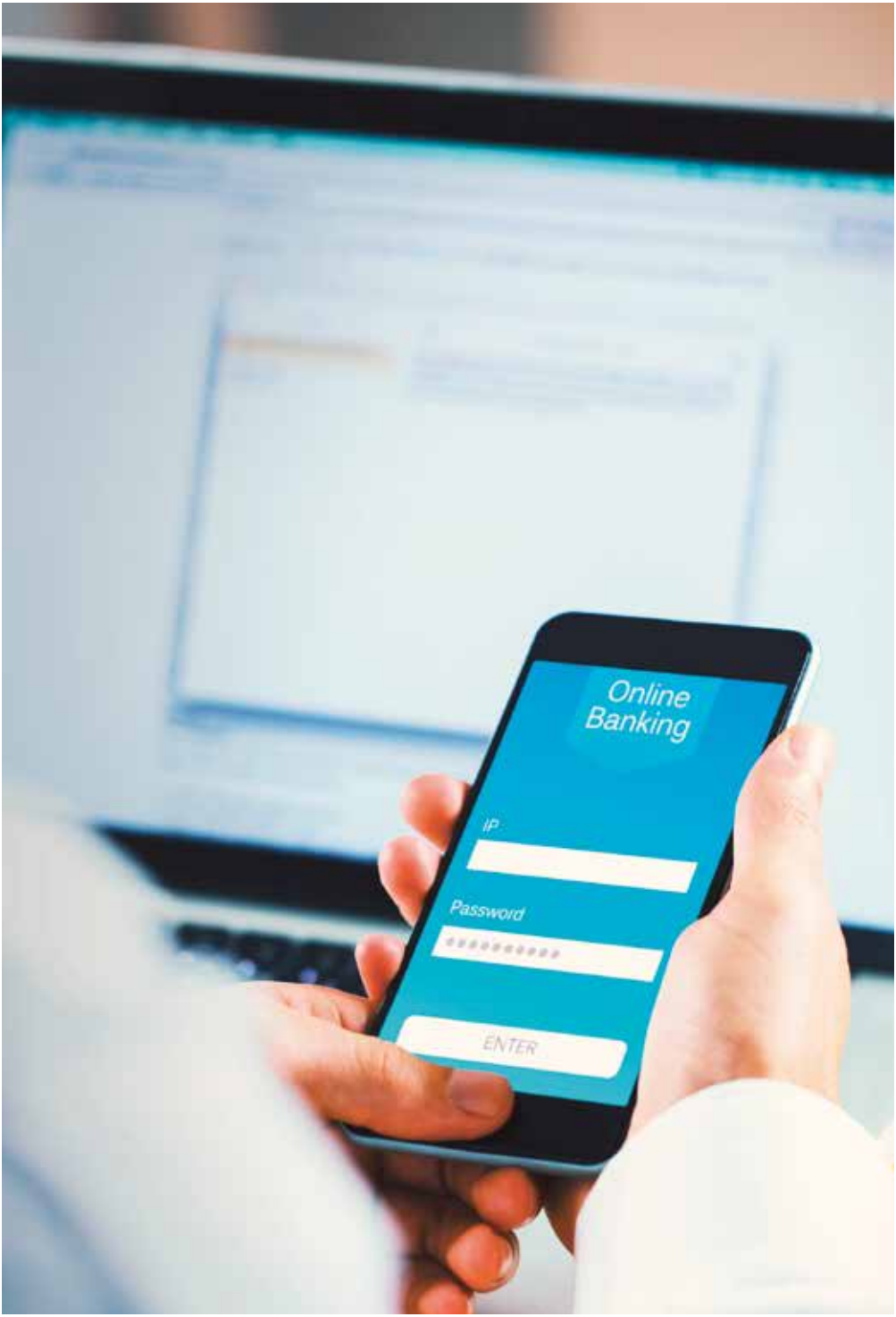
Wir haben bereits festgestellt, dass die Prävention ihre Grenzen hat. Die können technischer, finanzieller oder struktureller Natur sein. Im Extremfall kann sich ein Krimineller beispielsweise den Zugang zum Netz schlicht über die Bestechung eines Mitarbeitenden verschaffen. Wir müssen uns also eingestehen, dass wir erfolgreiche Angriffe erleben werden. Aufgabe der Detektion ist, diese frühzeitig zu erkennen. Typische Massnahmen dafür sind etwa:

- Data Leakage Prevention: Darunter versteht man die Detektion (und Prävention) unerwünschten Datenabflusses.
- Security Information & Event Management (SIEM): Hier geht es um die Korrelation von System Events zur Erkennung von Angriffen. Wir werden später sehen, dass dem SIEM heute Grenzen gesetzt sind – deshalb ist der nächste Punkt besonders wichtig.
- Threat Intelligence: Sie sammelt auf breiter Basis Informationen und wertet sie zur Früherkennung von Angriffen aus.
- Honey Net: Darunter versteht man ein geschäftlich nicht genutztes Netz, das aber von aussen produktiv aussieht. Sobald dort Verkehr aufschlägt, ist wahrscheinlich ein Angriff im Gange.
- Datenaustausch mit Dritten.
- Weiteres, je nach Organisation und Infrastruktur.

6.4 Intervention

Leider passiert es oft, dass Firmen viel Zeit und Geld in die Detektion investieren und bei einem Vorfall dann nicht wissen, wie sie reagieren wollen. Damit die Intervention wirkt, muss sie aber schnell, effizient und effektiv sein. Dabei sollte sie möglichst das Geschäft nicht beeinträchtigen.

Bei der Intervention geht es vor allem darum, Prozesse zu definieren – aber natürlich nicht nur. Grundsätzlich gilt: Die Prozesse der Intervention müssen dokumentiert sein und auch gelebt werden. Nach einem Ernstfall kann auch die Nachvollziehbarkeit der getroffenen Massnahmen wichtig sein, damit der Vorfall im Nachgang aufgearbeitet werden kann. Dies ist erfahrungsgemäss nicht eben eine Stärke der beteiligten Parteien.


Online
Banking
IP
Password
ENTER

7 Was bedeutet das für ein Unternehmen?

Nachdem wir die Aktionsfelder und Möglichkeiten der Sicherheit betrachtet haben, stellt sich die Frage, was es für ein Unternehmen bedeutet, ein zeitgemässes Sicherheitskonzept zu leben. Dies lässt sich anhand dreier Teilgebiete diskutieren:

> Was bedeutet dies für die Sicherheitskultur?
> Wie kann Sicherheit strategisch gesteuert werden?
> Was bedeutet dies für die Sicherheitsorganisation?

Bei Swisscom ist das Vertrauen in die Mitarbeitenden ein zentraler Wert, der auch entsprechend gelebt wird. Die Sicherheit baut darauf auf, indem sie voraussetzt, dass die Mitarbeitenden grundsätzlich im Sinne des Unternehmens und der Kunden handeln wollen.

Es ist die Aufgabe der Sicherheitsorganisation, dieses Verhalten konstruktiv zu unterstützen. Sie hilft den Mitarbeitenden, ihre Aufgaben effizient und sicher zu erledigen. Dabei gilt es unbedingt zu vermeiden, dass die Mehrheit nach einem Vorfall für das Fehlverhalten einer Minderheit bestraft wird. Unsere Sicherheitskultur verlangt auch nach einem engmaschigen Monitoring für die wirklich kritischen Informationen. Und sie setzt voraus, dass ein Fehlverhalten rasch und effektiv sanktioniert wird.

7.1 Die Sicherheitskultur

Ein Unternehmen, das seine (Daten-)Sicherheit nachhaltig stärken will, braucht vor allem eine entsprechende Sicherheitskultur. Wer eine solche schaffen will, sollte beherzigen, dass Sicherheit in erster Linie den Menschen dienen und sie nicht behindern soll. Die Sicherheitsorganisation soll als Begleiter wahrgenommen werden, der Risiken transparent kommuniziert und das Business gleichzeitig wirksam unterstützt. Damit wird die Sicherheitsorganisation zur Partnerin, die Menschen hilft, ihre Arbeit in einer sicheren Art und Weise zu erledigen. In einer solchen Kultur kann sich Sicherheit als zentraler Gedanke nach und nach im Handeln der Mitarbeitenden etablieren.

In der Realität sind wir davon freilich noch weit entfernt. Wer heute von IT-Sicherheit spricht, meint damit zu oft noch die Konditionierung der Mitarbeitenden. Training, Förderung der Awareness und Kommunikation sind zweifellos wichtige Aufgaben, die es wahrzunehmen gilt. Sie sind aber eben nur ein Teil des Ganzen. Versteht sich eine Sicherheitsorganisation vor allem als Polizei im Unternehmen, darf sie sich nicht wundern, immer erst dann gerufen zu werden, wenn bereits ein Ereignis vorgefallen ist. Besser wäre es, als Dienstleister aufzutreten. Dann fielen viele Widerstände und Missverständnisse von vornherein weg. Das bedingt aber oft eine komplette Änderung der eigenen Sicht- und Arbeitsweise, also eine Anpassung der Kultur innerhalb der Sicherheitsorganisation selbst.

Human Centered Security

Ein Konzept, wie oben beschrieben, liesse sich unter dem Begriff Human Centered Security zusammenfassen. Hier übernimmt die Sicherheitsorganisation die Rolle eines internen Dienstleisters, der nach allen Seiten wirkt und vermittelt (Bild 4). Ihre Aufgaben lassen sich grundsätzlich in zwei Bereiche unterteilen: die Bereitstellung der Sicherheitsbasis und die Durchführung von Sicherheitsprojekten.

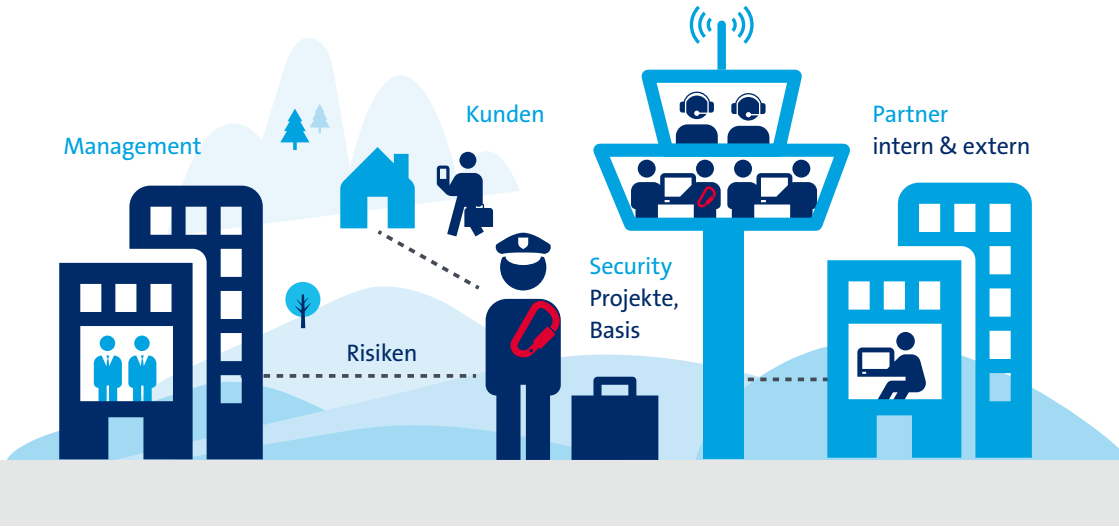


Bild 4: Konzept einer Human Centered Security. Der Co-Pilot repräsentiert die Aufgaben der Sicherheitsorganisation.

Die Sicherheitsbasis

Zur Basis gehören die fundamentalen Aufgaben und Prozesse der Sicherheitsorganisation. Wichtig ist, dass den Klassikern wie Security Policies und Governance, Training, Awareness, Kommunikation auch ein solides, akzeptiertes und gelebtes Risiko-Management zur Seite gestellt wird. Ansonsten läuft die Sicherheitsorganisation Gefahr, dass in den anderen Bereichen (vor allem bei Projekten) Entscheide getroffen werden, die zu inakzeptablen Risiken und Gefahren führen. Wie sich das vermeiden lässt, ist in Kapitel 7.2 skizziert.

So wichtig die Basis auch ist – sie besteht oft aus hochstandardisierten Prozessen, die so effizient und kostengünstig wie möglich abgewickelt werden sollen. Viele Aufgaben haben einen standardisierten Input, klare Tasks und einen standardisierten Output. Damit eignen sie sich für Prozesse, die so weit wie möglich optimiert und automatisiert werden sollen. Dies gilt speziell für die Prozessschritte, die keine wirklichen Werte generieren – also etwa für solche, in denen bloss Informationen von einer Tabelle in eine andere kopiert werden.

Zu guter Letzt sollen solche Prozesse auch gemessen und gemanagt werden. Dies ist auf den ersten Blick relativ einfach und kann, soll und wird Teil einer Score Card für die Sicherheit und die Prozesse sein. Die Messgrösse ist hier der Key Security Indicator (KSI). Er bezieht sich im Gegensatz zum betriebswirtschaftlichen Key Performance Indicator (KPI) ausschliesslich auf die Sicherheit. Jede Firma muss für den KSI ihre eigenen Messgrössen finden und als Score Card definieren. Wirklich schwierig dabei ist es, aussagekräftige Grössen aus dem Betrieb zu erhalten, die von der Geschäftsleitung auch verstanden werden.

Bei Swisscom werden die wichtigsten Prozesse durch sogenannte Procedures definiert. Wir haben uns entschieden, nicht breite und komplexe Prozesse aufzuzeichnen, sondern uns hierbei auf den Normalfall zu konzentrieren. Eine Procedure füllt nicht mehr als ein A4-Blatt und zeigt typischerweise die wichtigsten fünf bis acht Schritte. Dabei wird jeder Schritt nach RASCI (Responsible, Accountable, Supportive, Consulted, Informed) kategorisiert, womit auch die Verantwortlichkeiten klar geregelt sind. Zusätzlich werden die Ziele sowie der In- und Output festgelegt.

Diese Procedures haben sich als ein sehr effizientes Instrument bewährt. Eine Procedure kann im Rahmen eines Workshops meist in 30 bis 60 Minuten definiert werden. Das hilft den Teams gleichzeitig, sich selbst Klarheit über die Abläufe zu verschaffen. Des Weiteren sollen dabei Messgrössen definiert werden, die es erlauben, die Prozess-Effizienz zu messen und zu steuern. Wir haben bis jetzt rund 30 solcher Procedures geschrieben. Mit diesem Ansatz konnten wir die Effizienz gewisser Prozesse teilweise um das Drei- bis Vierfache verbessern. Dies hat dazu geführt, dass wir Kapazitäten freilegen konnten, um andere, oft auch spannendere Aufgaben zu erledigen.

Projekte

Die Sicherheitsorganisation soll Projekte von Anfang an effizient und zielgerichtet begleiten. Nur so kann sie sicherstellen, früh mit dabei zu sein und mithelfen zu können, Lösungen für die Probleme des Business zu finden. Hier muss sie sich aber von der reinen Compliance-Arbeit verabschieden. Es zeugt von keiner guten Kultur, wenn sie zu Projektanfang den Beteiligten bloss erklärt, welche Regeln sie einhalten müssen und zum Ende wieder auftaucht, um zu kontrollieren.

Dies kann genügen bei Projekten mit geringem Sicherheitsrisiko oder solchen, bei denen «Standard-Sicherheit» reicht. Bei allen anderen aber ist dies der falsche Ansatz. Ein Geschäftsbereich startet ein Projekt ja, um ein Problem zu lösen oder ein neues Geschäftsfeld zu erschliessen. Eine Sicherheitsorganisation, die sich als Dienstleisterin versteht, wird hier mithelfen, diese Ziele zu erreichen – und dabei natürlich auch als Hüterin der Sicherheit wirken.

Um eine solche Haltung zu fördern, können innerhalb der Sicherheitsorganisation beispielsweise kleine Teams mit Querschnittsaufgaben gebildet werden. Sie arbeiten dann eigenverantwortlich am Projekt und werden an dessen Erfolg gemessen. Wenn in einem solchen Team die wichtigen Security-Rollen vertreten sind – Governance, Architektur, physische Sicherheit, Monitoring –, können Entscheide vor Ort getroffen werden. So kann dem Projekt bei Bedarf rasch geholfen werden. Damit solche Entscheide aber im Sinne des Gesamtkontextes getroffen und dabei keine untragbaren Risiken eingegangen werden, erfordert es ein solides und stabiles Risiko-Management.

Im Geschäftsalltag hat sich gezeigt, dass die Querschnittteams mit ihrer Doppelrolle hin und wieder Mühe haben. Der Spagat, im Projekt einerseits die Governance zu vertreten und andererseits inhaltlich mitzugestalten, kann zu Identifikationsproblemen führen. Hier gilt es, das System so auszugestalten, dass es zwar durchlässig ist, aber auch konkrete Orientierungshilfen bietet.

Soviel zu den prinzipiellen Rollen in einer Sicherheitsorganisation. Selbstverständlich gibt es in diesem Zusammenhang viele Schnittstellen, die definiert und beachtet werden müssen. Auf die wichtigsten gehen wir im Folgenden kurz ein.

Was das Management braucht

Mittlerweile ist in vielen Konzernleitungen und Verwaltungsräten akzeptiert, dass Sicherheit ein Thema für die oberste Führungsetage ist. Wie aber sollen diese Gremien die Sicherheit steuern? Grundsätzlich ist die Antwort relativ einfach: Über ein Instrument, dessen sie sich im normalen Geschäftsalltag auch bedienen: das Risiko-Management. Aber genau da liegt oft die Schwierigkeit. Die Sicherheitsorganisation macht dem Management das Leben nämlich oft unnötig schwer, indem sie eine Komplexität und eine Wichtigkeit auf dieses Thema projiziert, die unnötig ist.

Risiken werden von Sicherheitsorganisationen häufig überschätzt. Ein grosser Teil der Risiken, die täglich bearbeitet werden, erreicht kaum die Grösse, die es braucht, um auf die Top-Liste der Unternehmensleitung zu gelangen – und das ist richtig so. Oft werden Risiken auch nicht stufengerecht kommuniziert. Bevor man den monatlichen Bericht für die Unternehmensleitung schreibt, sollte man sich zuerst fragen, welche Risiken dort wirklich relevant sind. Danach gilt es, die Auswirkungen von Sicherheitsvorfällen in diesen Kontext zu stellen. Selbstverständlich gibt es Risiken, die zwingend bis zum CEO kommuniziert werden müssen, aber das sind (hoffentlich) meist weniger, als man denkt. In diesem Fall geht Qualität vor Quantität.

Ein weiterer heikler Punkt ist die Frage nach den projizierten, finanziellen Auswirkungen eines Sicherheitsrisikos. Es gibt zwar verschiedene Formeln und Ansätze zum Quantifizieren von Risiken. Solange dabei keine Finanzzahlen mit im Spiel sind, können sie durchaus sinnvolle Ergebnisse liefern. Formeln können dabei helfen, Risiken zu priorisieren. Versucht man aber nur den finanziellen Schaden eines realen Vorfalls zu berechnen, wird man scheitern. So ist es beispielsweise unmöglich, einen Vertrauens- und damit Kundenverlust in Franken umzurechnen. Wenn das schon beim realen Vorfall nicht geht, wie soll es dann bei «blossen» Risiken möglich sein? Leider wird es gelegentlich trotzdem versucht, etwa um der Sicherheit virtuell mehr Gewicht zu verleihen. Meist kommt dabei aber genau das Gegenteil heraus, weil die Sicherheitsorganisation dadurch an Vertrauen verliert und fortan von der Geschäftsleitung nicht mehr als Partner auf Augenhöhe wahrgenommen wird.

Fazit: Die Sicherheitsorganisation soll Risiken gegenüber dem Management klar, offen und transparent kommunizieren ohne zu dramatisieren. Nur so können die Unternehmensbereiche ihre Verantwortung bei der Sicherheit wahrnehmen.

Partner

Eine Sicherheitsorganisation hat verschiedene Partner – interne und externe. Insbesondere den Externen gilt es, die Risikobereitschaft, die Strukturen und die Kultur im Unternehmen zu vermitteln.

Bei Swisscom versuchen wir die Zahl der Partner in einer vernünftigen Grösse zu halten, dafür aber engere Beziehungen zu ihnen aufzubauen. Das ermöglicht es den Partnern, zu verstehen, wie unser Unternehmen funktioniert und welche Spielregeln bei uns gelten. Dies erleichtert die Zusammenarbeit bei Beratungsaufgaben und hilft speziell auch bei Audits. In diesem Umfeld wollen wir oft eine Aussenmeinung einholen, und das verlangt nach einer engen Beziehung. Es kann sogar so weit gehen, dass wir Joint Ventures bilden.

Bei internen Partnern verhält es sich naturgemäss anders. Neben dem Business, das je nachdem eher als Kunde denn als Partner betrachtet wird, sind die Entwicklung und der Betrieb die wichtigsten Stakeholder. Sie sind letztlich zentral, wenn Sicherheit wirklich umgesetzt werden soll. Auch soll die Sicherheitsorganisation nicht mit erhobenem Zeigefinger agieren, sondern aktiv Mehrwerte schaffen. Man darf getrost davon ausgehen, dass niemand bewusst unsichere Umgebungen baut und/oder betreibt. Wenn jedoch das Business die Anforderungen nicht versteht oder die Sicherheitsorganisation die Probleme von Betrieb oder Entwicklung verkennt, wird kaum eine echte Partnerschaft entstehen. Gefragt sind also eine gut Kommunikation, Empathie und ein konsequentes Risiko-Management.

Wir versuchen vehement, Lösungen gemeinsam mit dem Business, der Entwicklung und dem Betrieb zu finden. Dabei gibt es offensichtlich Anforderungen, die nicht verhandelbar sind. Dazu zählen solche, die vom Gesetz oder von Verträgen vorgegeben, aber auch solche, die schlicht eine Frage der Security Good Practice sind. In letzteren Fällen ist die Sache klar, und die Sicherheitsorganisation fühlt sich zuständig und zu Hause. In allen anderen Fällen gibt es aber verhandelbare Grauzonen. Die sollen für die Suche von kreativen Lösungen auch genutzt werden. Voraussetzung ist aber, dass der Risiko-Owner das Risiko versteht, es akzeptieren kann und die Sicherheitsorganisation damit einverstanden ist.

Ein typisches Beispiel ist das Patch Management. Auch bei Swisscom gibt es den Konflikt zwischen Sicherheitsorganisation («Wir müssen diesen Patch sofort ausrollen, weil die Schwachstelle höchst kritisch ist!») und dem Betrieb («Never touch a running system!»). In solchen Fällen wird gemeinsam nach Lösungen gesucht und auf Basis des objektiven Common Vulnerability Scoring System (CVSS) auch gefunden. Beim CVSS werden drei Bereiche transparent bewertet:

Base: beschreibt die grundlegenden Metriken einer Schwachstelle und deren Einfluss auf die Verfügbarkeit, Integrität und Vertraulichkeit eines Systems.

Temporal: umfasst Metriken, die sich über die Zeit ändern können (etwa die Qualität und Verfügbarkeit von Schadsoftware), die aber unabhängig vom Unternehmen und somit universell gültig sind.

Environmental: beschreibt die Schwachstelle im Kontext des Unternehmens. Diese Aufteilung erlaubt es der Sicherheitsorganisation, die ersten beiden Parameter zu bestimmen. Den dritten übernimmt idealerweise der Betrieb. So lässt sich effizient und anhand eines objektiven Bewertungssystems gemeinsam entscheiden, ob ein Patch rasch ausgerollt werden muss oder in den nächsten, regulären Release-Zyklus integriert werden kann.

Unsere Erfahrung zeigt, dass auf diese Weise oft pragmatische Lösungen entstehen, die für alle Beteiligten tragbar und akzeptabel sind. Vor allem kann hier nachvollziehbare Transparenz geschaffen werden, wo früher Risiken über- oder unterbewertet wurden. Wichtig ist aber, dass die Frage, ob ein Risiko akzeptabel ist, auf der richtigen Managementstufe beantwortet wird. Und: Die Sicherheitsorganisation muss wirklich dahinterstehen können.

Kunden

Die Kunden sollen für die Sicherheitsorganisation immer im Zentrum stehen – egal ob interne oder externe. Speziell in der ICT-Branche gehören hier auch Kunden des eigenen Unternehmens dazu, die irgendwie von der Sicherheit betroffen sind. Dies gilt sogar dann, wenn sie mit der Sicherheitsorganisation selbst nichts zu tun haben. Selbstverständlich gibt es auch andere Stakeholder – speziell im Umfeld kritischer Infrastrukturen hat zum Beispiel die Bevölkerung ein starkes Interesse an einer professionell umgesetzten Sicherheit.

Bei Kunden geht es immer auch um Menschen. Ihnen soll ermöglicht werden, ihre Aufgaben einfach, zielgerichtet und sicher zu lösen. Deshalb ist es wichtig, dass die Belange der Sicherheit einfach zu begreifen und transparent sind. Eigentlich soll es den Nutzer eines Systems nicht kümmern, wie die Informationen geschützt werden – es soll einfach geschehen.

Ein typisches Problem, das viele Firmen kennen: Es werden vertrauliche Informationen über Dropbox, Box, OneDrive und dergleichen ausgetauscht. Die Mitarbeitenden nutzen solche Dienste ja nicht aus bösem Willen, sondern aus Mangel an Alternativen. Will eine Sicherheitsorganisation dies in den Griff bekommen, sollte sie sich fragen, wie Mitarbeitende auf einfache und zuverlässige Weise grosse Dateien zu externen Lieferanten und Partnern transferieren können. Welcher Art sind die Dateien? Sollte das Unternehmen selbst eine gut handhabbare Option anbieten oder kann man eine Lösung einkaufen?

Wenn die Sicherheitsorganisation mit solch einer Haltung an das Problem herangeht, wird sie viel an Transparenz gewinnen. Dabei wird auch rasch klar, wo die Risiken wirklich liegen: Nur, weil eine Policy den Einsatz von Dropbox und ähnlichen Diensten verbietet, heisst das noch lange nicht, dass sich alle daran halten. Das Einzige, was man damit erreicht, ist, dass die Sicherheitsorganisation im Ernstfall rasch einen Schuldigen hat...

Ein Ziel der Sicherheitsorganisation von Swisscom ist, die Sicherheit so auszugestalten, dass sie die Nutzer möglichst einfach handhaben können. In diesem Zusammenhang wird beispielsweise eine einfache, schlanke und pragmatische Policy zu BYOD erarbeitet. Wenn diese Policy einmal verabschiedet ist, wird die Sicherheitsorganisation intensiv darüber nachdenken, wie sie einfach an die Mitarbeitenden gebracht werden kann. Wie zum Beispiel lässt sich die Policy gestalten, dass es Spass macht, sie zu lesen?

Zusätzlich suchen wir auch nach einer Technik, die zum Beispiel die Authentisierung und die Verschlüsselung für die Nutzer deutlich vereinfacht. Wenn wir in der Lage sind, diese beiden Aufgaben zu lösen, werden wir auch beim BYOD die Risiken nachhaltig adressieren können. Das Kapitel 8.1 zeigt, wie wir das angehen wollen.

7.2 Die Sicherheitsorganisation als Copilot

Aus den bisherigen Überlegungen lässt sich nun die Rolle der Sicherheitsorganisation in einem Unternehmen ableiten. Über allem steht hier der Grundsatz, dass sich die Sicherheitsorganisation ständig, konsequent und zielgerichtet weiterentwickeln muss, um der Sicherheit intern eine angemessene Stellung zu sichern.

Die Kernaufgabe der Geschäftsbereiche ist es, die Geschäftsstrategie zu entwickeln. Die Sicherheitsorganisation wiederum hat zur Aufgabe, die Geschäftsbereiche bei der Umsetzung der Strategie zu unterstützen und die Risiken in einem vertretbaren Rahmen zu halten. Mit anderen Worten: Wohin die Reise geht, wohin der Flieger fliegt, entscheidet das Business. Die Sicherheitsorganisation sorgt dafür, dass die grössten Gewitter um- und die Berge in sinnvoller Höhe überflogen werden. Dazu muss sie natürlich wissen, wo diese Gewitter und Berge sind.

Bild 5: Die Sicherheitsorganisation hilft, das Flugzeug sicher an Gewittern und Bergen vorbeizumanövrieren.

Policy und Governance

Traditionell konzentrierte sich die Sicherheit sehr auf die Policies und die Compliance. Basierend auf Good Practice wurden Richtlinien erarbeitet und implementiert. Danach versuchte man nachzuprüfen, wie gut sie eingehalten werden. Von ihrem Umfeld wurde die Sicherheitsorganisation deshalb als eine Art Polizei im Unternehmen wahrgenommen. Zwar wussten die Fachleute, dass Policies oft schwer zu verstehen und damit auch schwer einzuhalten sind. Bekannt war auch, dass Policies die Mitarbeitenden gelegentlich bei der Ausübung ihrer Aufgaben im Weg standen, aber bessere Alternativen wurden lange nicht angeboten.

Heute weiss man: Policies und Governance sind zwar zentrale Aspekte der Sicherheit, sie müssen aber die richtige Balance zwischen den Anforderungen der Sicherheit und jenen des Business wahren. In diesem Umfeld gilt es, eine gute und solide Arbeit abzuliefern – in Partnerschaft mit den Geschäftsbereichen und den anderen Stellen innerhalb der Sicherheitsorganisation.

Monitoring und Review

Grundsätzlich sollte in Unternehmen eine Kultur gelebt werden, die voraussetzt, dass sich Mitarbeitende korrekt und loyal verhalten. Eine solche Kultur des Vertrauens soll sich auch in der Sicherheitsstrategie niederschlagen, freilich, ohne dabei naiv nur an das Gute im Menschen glauben zu müssen.

Wie im Luftverkehr soll die Sicherheitsorganisation den Betrieb und die Projekte kontinuierlich überwachen und Abweichungen erkennen. Dazu muss sie in den Steuerungsgremien, insbesondere der Projekte, vertreten sein und eine aktive Rolle spielen, wenn es um die Erreichung von Meilensteinen und Prüfpunkten geht.

Bild 6: Die Sicherheitsorganisation sollte den Betrieb und die Projekte kontinuierlich überwachen und Abweichungen erkennen.

In Projekten
Lösungen, nicht Probleme schaffen

Bereiche
Security Officers sind strategische Partner

Bild 7: Ein Security Officer soll sich mit den Zielen des Business identifizieren können.

Kundenbegleitung

Die Policies geben den Rahmen vor, die Überwachung deckt Verletzungen der Richtlinien auf. Währenddessen sorgt die angemessene Begleitung der Kunden (internen und externen) durch die Sicherheitsorganisation dafür, dass Fehltritte möglichst gar nicht passieren. Eine erfolgreiche Kundenbegleitung braucht Consultants und Security Officers, die den Kunden einen Mehrwert liefern. Das heisst etwa: Sie identifizieren sich mit den Projekten und sind daran interessiert, sie erfolgreich und sicher abzuwickeln. Die Security Consultants sollen sich also für den Erfolg des Projektes mitverantwortlich fühlen.

Gleiches gilt für die Security Officers. Ihr Ziel muss es sein, dass das Business als Kunde seine Ziele auf einem sicheren Weg erreichen kann. Deshalb lassen sich die Security Officers auch am Geschäftserfolg ihres Bereiches messen.

Security – the place to be

All das lässt sich nur verwirklichen, wenn die Sicherheitsorganisation die richtigen Mitarbeitenden an Bord hat. Sie sollen motiviert den gemeinsamen Weg gehen und eine gemeinsame Überzeugung teilen. Hierfür müssen Rahmenbedingungen geschaffen werden, die die Sicherheitsorganisation zum «the place to be» für Top-Leute macht.

Um das zu erreichen, gibt es verschiedene Ansatzpunkte: Vor allem sollte die Sicherheitsorganisation in der Firmenhierarchie möglichst weit oben und unabhängig vom Betrieb angesiedelt sein. Dann vermittelt sie auch das Bild, wirklich etwas bewirken zu können. Das, was sie tatsächlich bewirkt, sollte sie dann quasi über geeignete Schaufenster bekanntmachen – intern wie extern. Hierfür eignen sich etwa regelmässige Security- oder Risiko-Management-Reports für Kunden und Partner. Nach innen helfen Sicherheits-Bulletins oder regelmässige Sitzungen mit der Firmenleitung, respektive dem Verwaltungsrat, die Sicherheitsorganisation ins rechte Licht zu rücken. Dass sie dabei stets auf dem Stand des Wissens und der Technik operiert, versteht sich von selbst, soll aber auch in geeigneter Form kommuniziert werden.

Stets das Ganze im Auge behalten

Hier gilt es noch anzumerken, dass jede noch so gut gelöste Security-Aufgabe für sich nur beschränkte Wirkung haben wird. Egal, ob es sich um Policy und Compliance, Monitoring und Review, Projektbegleitung, Training oder andere Teilbereiche handelt: Die Massnahmen entfalten ihre volle Wirkung erst im Zusammenspiel. Das Ökosystem Sicherheit kann nur mit einem gemeinschaftlichen Ansatz gelebt werden. Wenn das alle verinnerlicht haben, wird sich die Sicherheitsorganisation ständig verbessern können und zum Gesamterfolg eines Unternehmens beitragen.

7.3 Strategische Steuerung

Die Sicherheit sollte auf zwei Ebenen gesteuert werden: Auf der einen Seite durch den strategischen Einsatz des Risiko-Managements und auf der anderen durch strukturierte Planung.

7.3.1 Risiko-Management

Die Erfahrung zeigt, dass Risiko-Management nur auf dem Papier einfach ist. Grundsätzlich sind die Prozesse klar und lassen sich in der Theorie auch präzise definieren. Leider wird die Theorie aber oft von der Praxis eingeholt. Risiken sind selten einfach zu erkennen und ihre Auswirkungen lassen sich kaum zuverlässig abschätzen.

Aber was ist eigentlich das Ziel des Risiko-Managements? Grundsätzlich sollte es einem Unternehmen ermöglichen, seine grössten Risiken zu kennen und aktiv zu bewirtschaften. Dabei sind die potenziellen finanziellen Auswirkungen sekundär. Klar wäre es interessant, die Risiken dem Aufwand für die Sicherheit monetär gegenüberzustellen. Aber in einer Kultur, in der Risiken transparent kommuniziert und aktiv bewirtschaftet werden, bringen aufwendige betriebswirtschaftliche Betrachtungen ohnehin nicht viel. Wichtiger sind qualitative Szenarien, die realistisch zeigen, was unter welchen Bedingungen wirklich passieren könnte.

Entscheidend ist der Prozess, der definiert, wie mit Risiken umgegangen wird. Aufgabe der Sicherheitsorganisation ist es, die Bedrohungslage zu kennen und darauf basierend Szenarien zu entwickeln, die es erlauben, Risiken zu erfassen und abzuschätzen. Die Geschäftsbereiche wiederum tragen den Grossteil der Risiken und müssen auch die Massnahmen zu deren Reduktion finanzieren.

Dabei ist wichtig, dass auf der richtigen Managementstufe entschieden wird, welche Risiken als akzeptabel angesehen werden und welche nicht. Die richtige Stufe ist in der Regel dort, wo die Person arbeitet, die nach einem Vorfall den Kunden erklären muss, warum er passiert ist. Bei grösseren Projekten wird also sinnvollerweise das obere Management involviert. Wenn dies in einem konstanten Dialog geschieht, dann kann ein sehr konstruktiver Prozess entstehen.

7.3.2 Das Security-Geschäftsjahr

Grundsätzlich soll sich die Planung der Sicherheitsorganisation am Rhythmus der Unternehmensplanung anlehnen. Wie das auf einer hohen Abstraktionsebene aussehen kann, zeigt Bild 8.

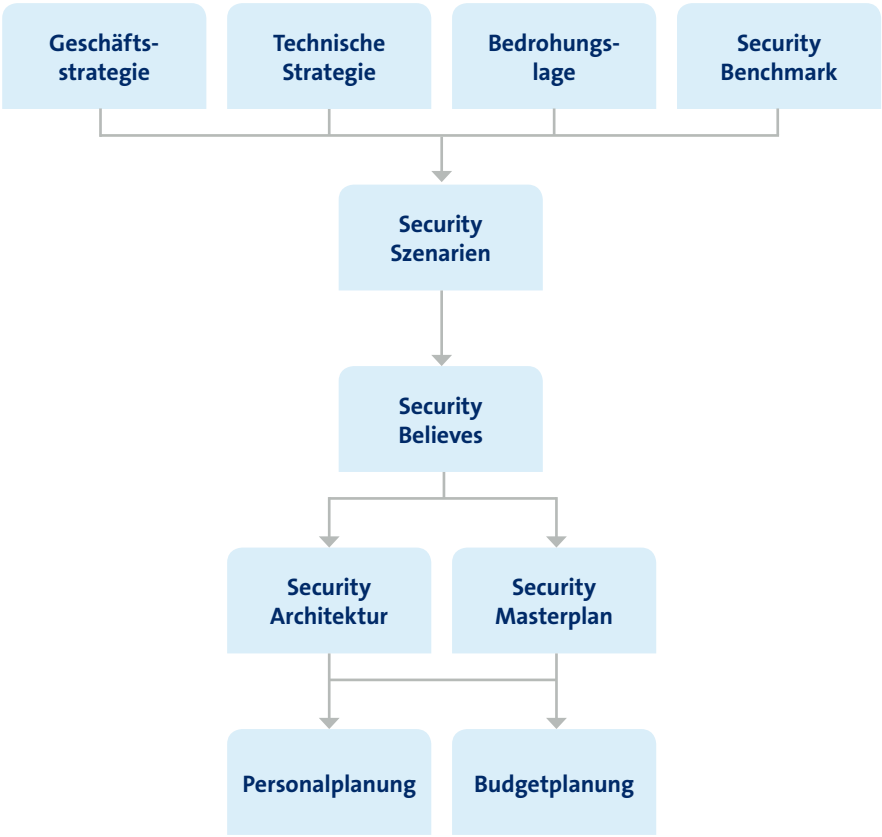


Bild 8: So könnte die Planung einer Sicherheitsorganisation aussehen, wenn sie mit der Geschäftsplanung gekoppelt wird.

Zu Beginn der Planung machen sich Unternehmen Gedanken über Strategie und Planung der nächsten Jahre. Dies muss auch die Basis für die Planung der Sicherheitsorganisation sein, da sie ja das Business unterstützen soll. Die Sicherheitsorganisation sollte auch in der Lage sein, dem Business gute Voraussetzungen hinsichtlich der IT zu schaffen. Unter Umständen sind hierfür bauliche oder architektonische Vorarbeiten zu erledigen. Dasselbe gilt natürlich für die technische Strategie oder für Architektur-Visionen, die als Basis für die Sicherheit dienen.

Von der Bedrohungslage…

Die Bedrohungslage muss klar umrissen und realistisch sein. Sie muss auch Aussagen über künftige Entwicklungen machen, da die Business-Planung in diesen Kontext gestellt und Geschäftsstrategien in diesem Umfeld geschützt werden. Die Sicherheitsorganisation sollte sich beim Vermitteln der Bedrohungslage klarer und einfacher Bilder bedienen, die von Business und Management verstanden werden. Wichtig ist, im ganzen Unternehmen von der gleichen Bedrohungslage auszugehen und einheitlich zu planen. Klar ist aber auch, dass Ereignisse alles wieder infrage stellen und Korrekturen verlangen können.

Natürlich wäre ein Benchmark zum Beurteilen der Sicherheitssituation sehr nützlich. Leider gibt es sehr wenig Material auf dem Markt, das als brauchbare Grundlage für eine neutrale und objektive Bewertung hinzugezogen werden kann. Nichtsdestotrotz soll auf der Basis bestehender Konzepte versucht werden, einen passenden Benchmark zu entwickeln. Interessant sind vor allem der ISF Benchmark und der ISF Healthcheck.

… über die Szenarien…

Aufbauend auf diesen Vorarbeiten lassen sich Szenarien bauen, die Hypothesen dazu liefern, wie die Welt in Zukunft aussehen könnte. Da keine eindeutigen Aussagen gemacht werden können, lohnt es sich, über verschiedene Szenarien nachzudenken. Das erleichtert es zu verstehen, wie die Sicherheitsorganisation das Geschäft unter verschiedenen Rahmenbedingungen erfolgreich unterstützen kann.

Aus den Szenarien werden die Grundsätze – sogenannte Believes – für das Unternehmen abgeleitet. Damit kann die Frage beantwortet werden, was beachtet werden muss und unter welchen Prämissen eine Architektur und ein Umsetzungsplan erstellt werden sollen.

... zur Sicherheitsarchitektur

Jetzt wird es endlich Ernst. Basierend auf den vorliegenden Informationen kann die Sicherheitsarchitektur eines Unternehmens überarbeitet (oder erst einmal erstellt) werden. Dabei zeigt sich, was vorgesehen werden muss, damit das Unternehmen (und auch die Sicherheitsorganisation) in den verschiedenen Szenarien erfolgreich sein kann. Zusätzlich erhält man Informationen darüber, wie die Believes am kostengünstigsten umgesetzt werden können. Ähnliches gilt für den Masterplan: Hier zeigt die Auseinandersetzung mit Szenarien und Believes grob, welche Projekte und Aufgaben umgesetzt werden müssen, um die Architektur weiterzubringen und erkannte Mängel (aus dem Benchmark) zu beheben, ohne die Stärken zu gefährden.

Dass daraus das Budget abgeleitet werden kann, ist offensichtlich. Interessant ist jedoch, dass sich die Diskussion darüber, wie viel ein Unternehmen für die Sicherheit bezahlen will, jetzt viel einfacher führen lässt. Die Herleitung ist ja nun klar und kann transparent kommuniziert werden. So wird den Beteiligten verständlich vermittelt, wo und warum etwas getan werden soll.

Was in vielen Firmen zu kurz kommt, ist die strategische Personalplanung. Dabei lässt sich aus Masterplan und Architektur gut ableiten, welches Know-how in Zukunft wie dringend benötigt wird, wo investiert oder devestiert werden soll.

Ist der beschriebene Planungsprozess durchschritten, beginnt alles wieder von vorn. Dieses Vorgehen erlaubt es, die Sicherheit strukturiert und strategisch zu steuern und proaktiv zu handeln. Entscheidend ist, dass die Sicherheitsorganisation bereits bei der Geschäftsstrategie mit einbezogen wird. Dabei hat sie aber vor allem eine zuhörende Rolle. Es geht nicht primär darum, die Strategie zu beeinflussen (man kann allenfalls auf Risiken hinweisen). Vielmehr lernt die Sicherheitsorganisation so, was sie beitragen kann, damit das Business seine Ziele erreicht. Mit einer solchen Grundhaltung rennt man dort oft offene Türen ein.

7.4 Organisatorisches

All die verschiedenen Ideen und Konzepte beeinflussen natürlich Sicherheitsorganisationen selbst und ihre organisatorische Einbettung. Dabei gibt es zwei Grundsätze, die zu beachten sind:

1. Sicherheit ist Chefsache – sie kann nicht delegiert werden und muss auf höchster Stufe angesiedelt sein. Nur so erhält das Top-Management ungefilterte Informationen und nur so kann die Sicherheit ihre volle Wirkung entfalten. Und am Ende sorgt dieses Konzept auch dafür, dass der CEO und die Mitglieder der Geschäftsleitung ihre Sorgfaltspflicht wahrnehmen können.

2. Integrale Sicherheit ist der Schlüssel zum Erfolg. Ein integrales Sicherheitskonzept kann leichter umgesetzt werden, wenn die verschiedenen Aufgaben wie Policies, Governance, physische Sicherheit, Architektur und CSIRT unter einem Dach zusammengeführt werden. So können auch unkonventionelle Lösungen gesucht werden, bei denen sich physische Schwächen allenfalls durch logische Massnahmen kompensieren lassen – oder umgekehrt.

Natürlich birgt dieser Ansatz auch Schwächen und Risiken. Wenn alle Sicherheitsfunktionen beim Top-Management zusammengeführt werden, besteht etwa die Gefahr, dass sich die Sicherheitsorganisation einen Elfenbeinturm baut. Dem muss Rechnung getragen werden.

Bei Swisscom hat der CEO entschieden, dass Sicherheit strategisch wichtig ist. Deshalb hat er den Chief Security Officer – bei Swisscom heisst er Head of Group Security – direkt in seine eigene Organisation integriert. Diese Stelle wurde daraufhin neu geschaffen und besetzt. Ursprünglich ging man davon aus, dass die zugehörige Organisation klein sein werde und vorwiegend Policy- und Governance-Aufgaben wahrnehmen soll. Im Lauf der Diskussionen haben sich aber die Vorteile einer zentralen Organisation herausgeschält. Als Folge davon wurde die Sicherheit direkt beim CEO zentralisiert.

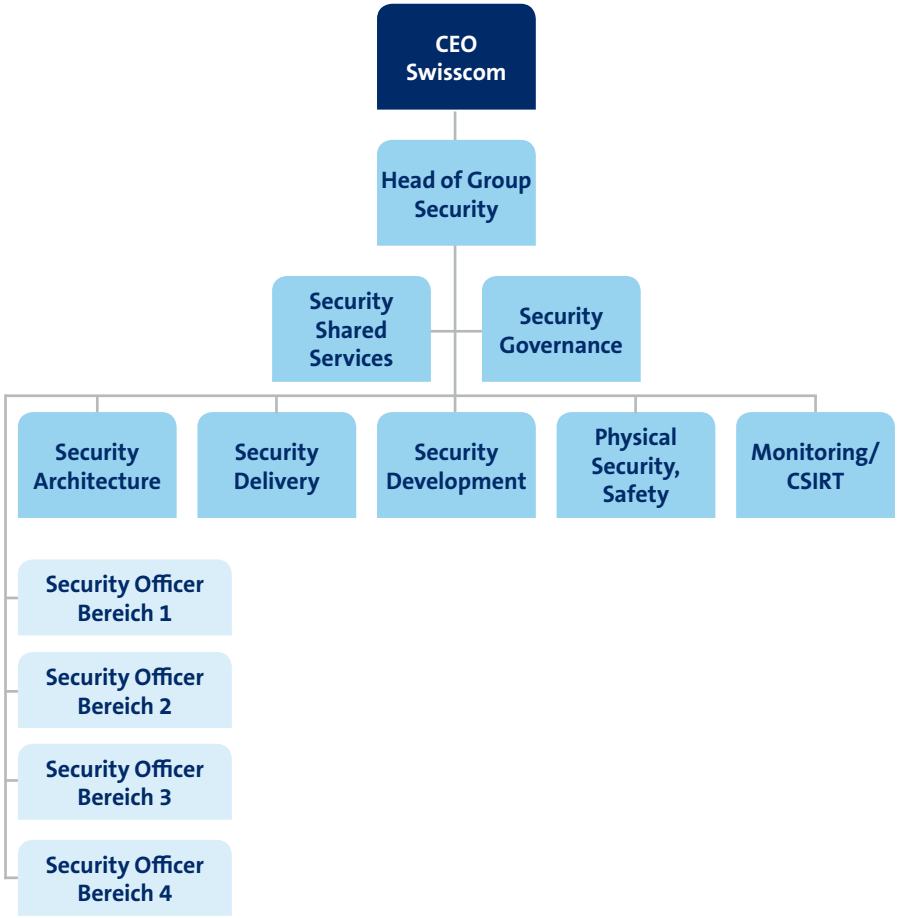


Bild 9: Das Organigramm zeigt die zentrale Bedeutung der Sicherheit bei Swisscom. Die gesamte Sicherheitsorganisation ist beim CEO angegliedert.

Der Head of Group Security berichtet an den CEO und ist Gast der Konzernleitung. Er wird bei Bedarf zugezogen oder kann bei Traktanden, die ihm wichtig erscheinen, jederzeit zur Konzernleitung stossen. So steht Sicherheit regelmässig auf der Traktandenliste der Konzernleitung und des Verwaltungsrates. Das schätzen beide Gremien insofern, als sie ständig über die aktuelle Bedrohungslage und ihre Entwicklung informiert werden. Zudem sind sie im Bilde, was hinsichtlich Sicherheit unternommen wird.

Die Sicherheitsorganisation selbst ist in einer klassischen Matrix organisiert. Sie besteht aus sieben Teams und vier Fachführungskräften:

Security Architecture – der Name ist Programm. Dieses Team ist verantwortlich für die Sicherheitsarchitektur des Unternehmens. Es definiert die Architektur nicht nur, sondern setzt sie auch um. Das Team ist auch dafür verantwortlich, dass die Architektur in den Projekten gelebt und umgesetzt wird. So kann sichergestellt werden, dass keine Elfenbeintürme gebaut werden. Security Architecture hat enge Schnittstellen mit dem Team Enterprise Architecture. Damit ist es sozusagen der verlängerte Arm der Architektur in die Sicherheit.

Security Delivery: Vereinfacht gesagt ist die Security Delivery das interne Consulting. Dieses Team wickelt Projekte ab (sofern sie von der Sicherheitsorganisation verantwortet werden) und unterstützt Business-Projekte. Es wird als klassische Consulting/Engineering-Organisation geführt und hat auch die entsprechenden Verantwortlichkeiten.

Secure Software Development: Dieses Team ist eine Folge davon, dass Software bei Swisscom immer wichtiger wird. Dieser Trend fusst auf dem wachsenden Bedürfnis der Geschäftsbereiche, Software selbst zu entwickeln, und das möglichst dezentral und agil. Er wurde vor allem durch das Aufkommen von App-Entwicklungen angestossen. Der Trend wird aber auch begünstigt durch die Forderung, schnell auf den Markt reagieren zu können – oder einen Markt überhaupt erst zu schaffen. Damit unter diesen Voraussetzungen Software entsteht, die Sicherheit bereits mit eingebaut hat, braucht es während der Entwicklung eine intensive Unterstützung durch die Sicherheitsorganisation. Im Weiteren entwickelt das Team auch die wichtige Reporting-Umgebung, welche die Einhaltung der technischen Controls auf den Servern misst.

Physical Security, Safety: Dieses Team ist verantwortlich für die Vorgaben im physischen Bereich und deren Umsetzung. Dabei gilt es aber auch, die IT-Sicherheit in die anderen Bereiche der Sicherheit zu integrieren und kreative Lösungen zu suchen, mit denen sich neue Produkte effizienter und kostengünstiger produzieren lassen. Eine typische Frage könnte hier sein, ob künftig für bestimmte Dienste überhaupt noch teure stationäre Rechenzentren nötig sind, oder ob dafür Container-Rechenzentren genügen. Weiter deckt das Team auch die Arbeitssicherheit ab, also die Massnahmen, mit denen wir unsere Mitarbeitenden schützen – speziell diejenigen, die gefährliche Arbeiten erledigen.

Monitoring/CSIRT: Die aktuelle und zukünftige Bedrohungslage verdeutlicht, dass die Detektion von und die Intervention bei Angriffen künftig immer wichtiger wird. Mit der Einbindung des CSIRT in die Sicherheitsorganisation kann der Kreis der Informationen geschlossen werden. Das, was wir bei Detektion und Monitoring lernen, kann direkt zurück in die Policies und in die Architektur einfliessen. Dabei ist klar, dass das CSIRT eine sehr enge Schnittstelle zum Betrieb pflegt und die Integration in die Betriebsprozesse fundamental wichtig ist. So soll ein Sicherheitsvorfall prinzipiell nicht anders behandelt werden als jeder andere betriebliche Vorfall – einzig der technische Lead ist in diesem Fall beim CSIRT und nicht im Betrieb. Dieses Konzept hat sich bei Swisscom soweit sehr bewährt.

In der Sicherheitsorganisation gibt es noch zwei Stabsstellen: Die erste nennt sich **Security Governance und Policies.** Bei diesem wichtigen und zentralen Team liegt die Verantwortung für das Policy Framework, die Security Governance, das Risiko-Management, das Krisen-Management und für sämtliche ISO-Zertifizierungen. Das Team arbeitet eng mit verschiedenen anderen Stellen wie zum Beispiel der Legal Compliance zusammen. So ist es in der Lage, viele der wichtigen Themen horizontal zu bearbeiten, sowohl bezüglich Hierarchie als auch Technik.

Security Shared Services: Diese zweite Stabsstelle wirkt sozusagen als Drehscheibe für die Belange der Security. Wenn Mitarbeitende Fragen an die Sicherheitsorganisation richten, dann landen sie normalerweise dort. Security Shared Services bearbeitet Querschnittprozesse wie Exception Management, Kommunikation oder Awareness. Weiter haben wir dort den Security-CIO etabliert, der uns hilft, die verschiedenen Tools und Software-Pakete, die wir für die Sicherheit einsetzen, zusammenzubringen und zu vernetzen.

Nun könnte man natürlich zu bedenken geben, dass eine Sicherheitsorganisation, die direkt beim CEO und in der Nähe der Konzernleitung positioniert ist, Gefahr läuft, sich einen Elfenbeinturm zu bauen. Deshalb haben wir die Rolle der **Security Officers** geschaffen. Sie betreuen die verschiedenen Bereiche der Sicherheitsorganisation und bilden die Schnittstellen zwischen ihr und dem Business. Die Security Officers arbeiten eng mit den jeweiligen Bereichsleitern aus den Businesses zusammen. Dabei geht es um verschiedene Belange: Auf der einen Seite sollen die wichtigsten Risiken transparent durch die Bereichsleitung bearbeitet oder akzeptiert werden. Das erfordert eine enge und vertrauensvolle Partnerschaft. Auf der anderen Seite ist es die Aufgabe der Security Officers, die Anforderungen des Business zurück in die Sicherheitsorganisation zu tragen. Dies sorgt dafür, dass sich die Sicherheit in die richtige Richtung entwickelt. Zu guter Letzt sind die Security Officers auch für die Projekte und Lieferobjekte der Sicherheitsorganisation in ihren Geschäftsbereichen verantwortlich. Sie haben also eine ähnliche Rolle gegenüber den einzelnen Geschäftsbereichen wie der Head of Group Security gegenüber der Konzernleitung. Das hat sich bisher sehr bewährt.

8 Was bedeutet das für die Technologie?

An dieser Stelle sollen drei Konzepte speziell herausgestrichen werden, die helfen, Bedrohungen nachhaltig zu bearbeiten.

8.1 Datenzentrierte Sicherheit

Wenn es um den Schutz von Informationen geht, wurden in der Vergangenheit vor allem der Datenträger und der Transportweg betrachtet. Typischerweise müssen bei vertraulichen Informationen sowohl der Datenträger als auch die Datenübertragung verschlüsselt sein. Das führt jedoch dazu, dass die Kontrolle über die Daten in dem Moment verloren geht, in dem sie beim Empfänger ankommen. Zudem kann die unkontrollierte Verteilung kritischer Informationen nicht verhindert werden, wenn man sich nur auf Datenträger und -übertragung konzentriert.

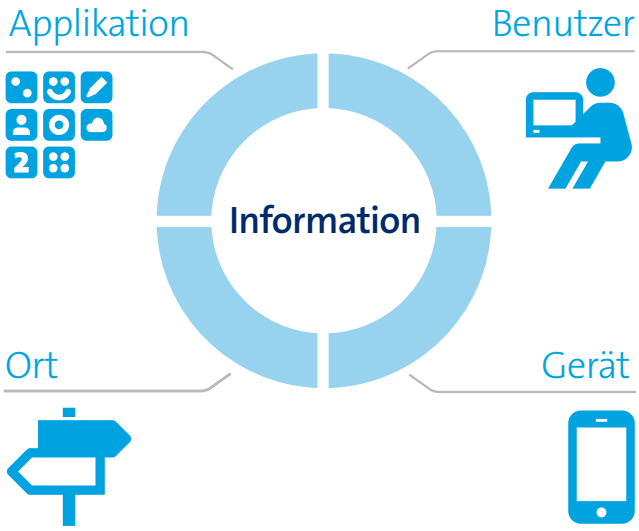


*Bild 10: **Wenn es um IT-Sicherheit geht, genügt es nicht, die Datenträger und die Übertragung zu verschlüsseln. Im Zentrum der Betrachtungen muss die Information selbst stehen.***

Dies muss sich ändern. Hierzu muss sich der Fokus vom Datenträger und Transport hin zur Information verlagern. Wichtig bei diesem Konzept ist, dass sich die Information selbst und persistent schützt. Mit anderen Worten: Die Information wird verschlüsselt und bleibt es, wohin sie sich auch bewegt. Einige Hersteller haben mit den Rights Management Services die Basis für einen solchen Ansatz gelegt, sind aber noch nicht den ganzen Weg gegangen.

Bei der datenzentrierten Sicherheit fällt die Information selbst den Entscheid über den Zugriff (oder technisch gesehen: ein Policy-Server) basierend auf vier Kriterien:

Der Benutzer: Hier geht es nicht nur darum, wer der Benutzer ist und welche Rolle er einnimmt, sondern auch, wie er sich authentisiert hat. Für öffentliche Kommentare auf einer Website kann es genügen, Facebook als Authentisierungsdienst zu verwenden. Bei firmeninternen Informationen können Benutzername und Passwort fürs Firmennetz reichen. Für vertrauliche Inhalte verlangt die Information aber nach einem zweiten Faktor wie einer Karte, einem Handy oder biometrischen Daten.

Das Gerät: Die Anforderungen an das Gerät hängen ebenfalls von der Datenklassifizierung ab. In vielen Firmen wird zwischen eigenen und Fremdgeräten unterschieden. Diese Unterscheidung ist aber prinzipiell nicht zweckmässig. Es geht einzig darum, ob das Gerät die Policy für den Zugriff auf die entsprechenden Daten erfüllt. Der Unterschied zwischen Geräten, die von der IT gemanagt und solchen, die von den Mitarbeitenden selbst gemanagt werden, liegt in der Verantwortlichkeit für die Erfüllung der Policy. Im ersten Fall ist die IT dafür zuständig, im zweiten der Mitarbeitende selbst. Anforderungen an das Gerät können Bedingungen enthalten wie Speicher-Verschlüsselung, Patch-Stand, Version des Betriebssystems etc.

Der Ort: Hinsichtlich des Orts gibt es zwei Ausprägungen. Die eine betrifft natürlich den geografischen Ort, an dem ein Rechner steht. Eine solche Sichtweise ist für die Finanzinstitute typisch. Dort darf auf bestimmte Daten nur innerhalb der Landesgrenzen zugegriffen werden. Je nach Genauigkeit könnte der Ort natürlich bis auf das Gebäude heruntergebrochen werden, in dem der Server läuft. Die zweite Bedeutung des Ortes basiert auf netzwerktechnischen Kriterien. Dabei könnte etwa unterschieden werden, ob sich der Rechner im Firmennetz befindet, ob er via VPN verbunden ist oder sogar in einem öffentlichen Netz steht.

Die Applikation: Auch die Applikation soll eine Rolle spielen. Ihre Version und ihr Patch-Stand kann die Entscheidung hinsichtlich des Datenzugriffs beeinflussen.

Als zusätzliches Kriterium könnte auch das Benutzerverhalten berücksichtigt werden. Dies praktiziert die Kreditkartenbranche in Form von Verhaltensanalysen ja bereits routinemässig. Sofern eine Technik zum Überwachen des Benutzerverhaltens von allen gängigen Geräten unterstützt würde, wären die Sicherheitsprobleme rund um BYOD weitgehend gelöst. Sollte ein Mitarbeitender das Unternehmen verlassen, kann der Zugriff sofort eingeschränkt oder verhindert werden.

Das Installieren von verhaltensbasierter Sicherheitssoftware auf privaten Geräten ist aber insofern problematisch, wie deren Support ja auch vom Hersteller oder vom «Laden um die Ecke» geleistet werden muss. Sollte die Sicherheitssoftware zu tief ins Betriebssystem eingreifen, wäre dieses Konzept hinfällig. Das Resultat wären hohe Supportkosten im Unternehmen oder aber viel Unzufriedenheit seitens der Mitarbeitenden.

Alles in allem darf man behaupten, dass eine konsequent umgesetzte, datenzentrierte Sicherheit viele Probleme löst. Sogar Cloud-Speicher wie Dropbox wären nur noch begrenzt ein Problem, da es eigentlich absolut irrelevant ist, wo sich die Daten befinden – sie sind geschützt. Public-Cloud-Angebote stellten ebenfalls keine Risiken mehr dar. Einzuschränken gilt es allerdings, dass die Suche in verschlüsselten Daten auch mit datenzentrierter Sicherheit nicht funktionieren wird.

Nun mag dieser Ansatz futuristisch scheinen. Es gibt jedoch schon einzelne Komponenten für eine solche Lösung und deshalb darf angenommen werden, dass der Weg durchaus gangbar ist.

8.2 Das Collaborative Security Model

Viele Unternehmen gehen generell davon aus, dass sich Sicherheitsvorfälle am zuverlässigsten erkennen lassen, wenn die jeweils besten Sicherheitsprodukte eingesetzt werden. Dies führt einerseits dazu, dass bei Detektion und Reaktion auf sehr unterschiedliche Konsolen und Techniken zurückgegriffen werden muss. Andererseits beruht die Entscheidung für das «beste» Produkt ja nur auf einer Momentaufnahme, die den Stand der Technik zum Zeitpunkt der Selektion abbildet. Dieser kann sich aber sehr kurzfristig wieder ändern.

Um diese Klippen zu umschiffen, hat Swisscom das Collaborative Security Model lanciert. Es nimmt sich beider oben erwähnten Schwächen an. Dabei geht es davon aus, dass die Geschäftsbereiche selbst bestimmen, welches Produkt sich momentan zum Lösen eines Problems am besten eignet. So können sie zum Beispiel für den Mail-Server den Virenschutz wählen, der gerade die beste Erkennungsrate liefert. Und so kann die erforderliche Sicherheitstechnik auch im Sinne eines «pay per use» lizenziert werden.

Weiter berücksichtigt das Modell, dass die meisten Firmen ihre Logs in einer Umgebung (Logging- & Monitoring-Plattform, Bild 11) zusammenfassen und sie auch für Sicherheitsauswertungen verwenden. Wenn sich die Logs dadurch umfassend konsolidieren lassen, kann die Detektionsrate für opportunistische Angriffe deutlich erhöht werden. Die Intervention bleibt aber nach wie vor kompliziert. Soll zum Beispiel ein Port gesperrt oder einem Rechner der Zugang zum Internet verwehrt werden, dann müssen die entsprechenden Regeln manuell bei den Proxy-Servern und/oder Firewalls konfiguriert werden. Dabei geht wertvolle Zeit verloren.

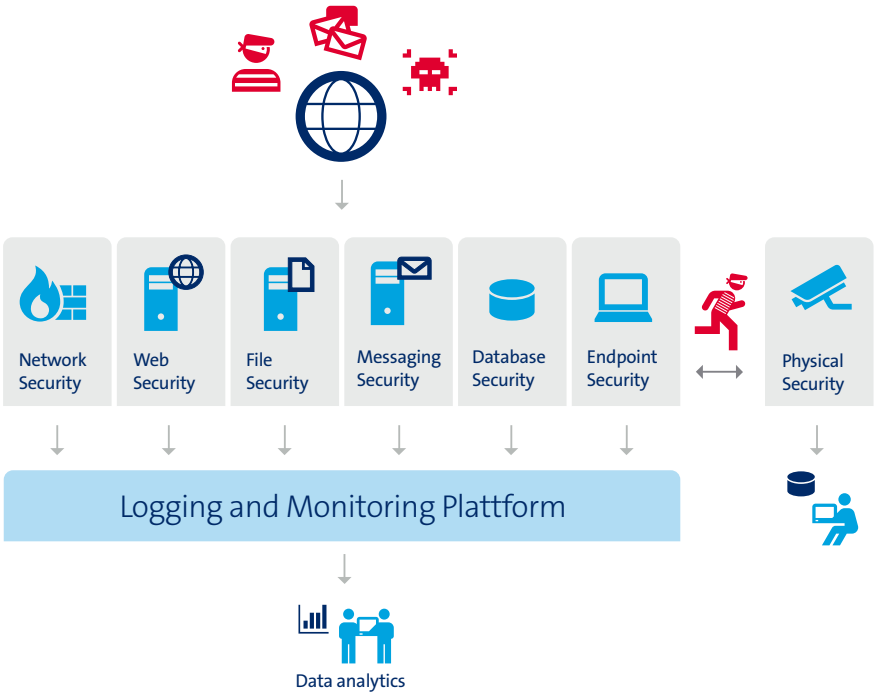


Bild 11: Das Collaborative Security Model gibt den Bereichen eine gewisse Freiheit bei der Wahl der Sicherheitslösungen und konsolidiert die Logs so, dass sie sich für regelmässige Sicherheitsauswertungen eignen.

Dieses Zeitproblem will Swisscom durch die Einführung einer zusätzlichen Abstraktionsschicht zwischen den Sicherheitsprodukten und der Logging- & Monitoring-Plattform lösen. Sie nennt sich Abstraction Layer (Bild 12) und wird zusammen mit dem Hersteller der Logging- & Monitoring-Plattform definiert und gepflegt. Die Abstraction Layer ermöglicht, dass Aktionen gegenüber den verschiedenen Security Layers direkt ausgelöst werden können. Obschon dieses Konzept noch in der Umsetzung steckt, hat sich schon gezeigt, dass es die Reaktionszeit deutlich zu verkürzen vermag.

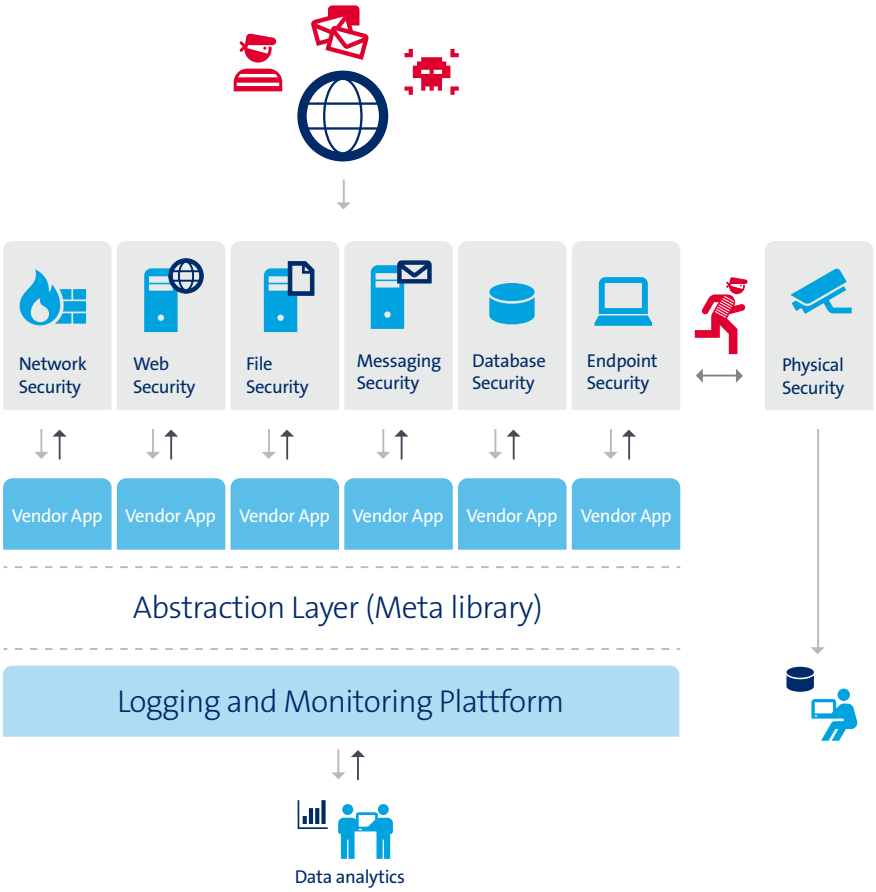


Bild 12: Konzept für eine Meta-Layer, die eine rasche Reaktion auf Angriffe erlaubt.

8.3 Threat Intelligence

Es wurde bereits darauf hingewiesen, dass die Detektion in Zukunft noch wichtiger wird. Dem liegt zugrunde, dass keine Prävention perfekt ist und Angriffe teilweise erfolgreich sein werden. Deshalb braucht es bei der Detektion neue Wege. Die heutigen Ansätze, die mit sogenannten «Security Information and Event Management (SIEM)»-Systemen verfolgt werden, haben sich nur begrenzt bewährt. Die Herausforderung bei diesen Systemen liegt darin, dass sie nur die Fragen beantworten können, die man bereits kennt. Das heisst: Es werden im Voraus Kriterien definiert, unter denen ein Alarm ausgelöst wird. Dieser Ansatz verursacht verschiedene Probleme:

> Er ist ausserordentlich statisch und eignet sich damit nur bedingt im Kampf gegen dynamische Angreifer.
> Er skaliert nur sehr begrenzt.
> Er benötigt gut ausgebildetes Personal, das schwierig zu finden ist.
> Er ist für den Angreifer vorhersehbar.
> Er ist oft komplexer, als man erwartet.

Es braucht also eine dynamische und weniger gut vorhersehbare Lösung. Leider gibt es zurzeit auf dem Markt keinen Ansatz, der direkt übernommen werden könnte. Da diese Konzepte und Ideen sehr neu sind, lassen sich hier noch keine allgemeingültigen Rezepte geben.

Bei Swisscom wurden bereits Teile einer dynamischen Detektion umgesetzt. Begonnen wurde mit zwei relativ einfachen Massnahmen:

1. Jede/-r Mitarbeitende im CSIRT hat offiziell eine gewisse Zeit pro Woche zur Verfügung, selbständig und nach eigenem Ermessen nach APTs (Advanced Persistent Threats) zu suchen. Erfahrene Analysten, die das Netzwerk kennen, haben durchaus gute Chancen, zu fühlen, wenn etwas ein bisschen verbrannt riecht. Auch wenn dieser Ansatz nicht sehr strukturiert scheint, hat er doch bereits einigen Erfolg gehabt und er wird trotz aller technischen Alternativen beibehalten.

2. Um bei Vorfällen alle Beteiligten auf denselben Informationsstand zu bringen, wird für jeden grösseren Vorfall ein eigener, persistenter Chatraum erstellt. In diesen werden die Mitarbeitenden, die nicht im CSIRT arbeiten, aktiv eingeladen, sofern der Vorfall für sie relevant ist. Das ermöglicht eine schnelle, transparente und konsistente Information, und die Dokumentation führt sich quasi von selbst nach. Und so fängt man das Problem auf, dass die Incident Handler oft nicht sehr motiviert sind, die Dokumentation à jour zu halten.

Im Weiteren haben wir damit begonnen, Big Data für die Detektion von Anomalien im Datenverkehr zu verwenden. Hierzu werden die Metadaten aus dem Verkehr im Firmennetz (keine Kundendaten!) eine bestimmte Zeit aufgezeichnet und dann ausgewertet. Weil Angriffe auf die IT oft nach ähnlichen Mustern ablaufen, können sie dabei erkannt werden. Wenn ein Muster bekannt ist, können die Sicherheitskomponenten entsprechend programmiert werden und dadurch weiteren Schaden verhindern.

8.4 Maturity Model

Klare Vorgaben in der Basis bleiben weiterhin ein wichtiger Eckpfeiler einer guten Sicherheit. Diese Vorgaben (Policies) reichen hinsichtlich Abstraktionsniveau von firmenweiten Richtlinien bis zur Umsetzung und Härtung jeglicher Objekte, die zur IT-Landschaft gehören, also Server, Workstations, Netzkomponenten, aber auch Applikationen, wie etwa Datenbanken.

In technischer Hinsicht ist ein über die Jahre gewachsenes und ausgereiftes Framework, basierend auf gängigen Standards wie dem Standard of Good Practice oder ISO, unentbehrlich. Dieses Framework nennt sich IT Security Level Basic (ITSLB) und beschreibt auf technischem Niveau, wie beispielsweise ein Objekt sicher konfiguriert sein muss. Dies ist aber nur eine Seite, die andere definiert, wie Patch Management, Malware Protection, IAM- und Proxy-Analysen aufgesetzt und gemanagt werden müssen. Der Deming-Regelkreis (nach William Edwards Deming, einem amerikanischen Physiker und Statistiker), der die Phasen «Plan», «Do», «Check» und « Act» umfasst, bildet das gesamte Maturity Model basierend auf dem ITSLB Framework ab.

Der Bereich «Plan» sowie Teile (technische Umsetzungsvorgaben – Fact Sheets) des Bereichs «Do» sind im ITSLB-Framework abgebildet. Die Umsetzung im Bereich «Do» wird dann durch den Betrieb verantwortet. Die Bereiche «Check» und «Act» werden mithilfe von Reportings und den daraus folgenden Behebungsmassnahmen abgedeckt.

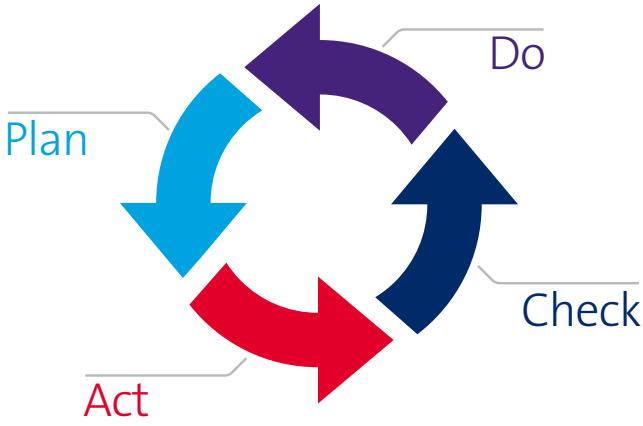


Bild 13: Der Regelkreis nach Deming bildet das gesamte Maturity Model basierend auf dem ITSLB Framework ab.

Wie sich zeigt, sind Endkunden, beispielsweise die eines Outsourcers, sehr interessiert an der Umsetzung der Sicherheit durch den Dienstleister. Für sie ist also der Bereich «Check» relevant. Von dort erhalten sie ein nachvollziehbares «Sicherheitsbarometer». Der Dienstleister braucht hierfür ein kundentaugliches Reporting. Dieses Reporting soll er aber auch für firmeninterne Zwecke verwenden, beispielsweise zum Einleiten von Behebungsmassnahmen.

Für die Überwachung der Maturity von internen und externen Nutzern hat Swisscom «Sophia» entwickelt. Sophia erlaubt, tagesaktuelle Informationen über Patch-Stand, Malware-Protection, ITSLB und weiteres via Web abzurufen. Genutzt wird es in erster Linie für die Serverlandschaft, aber auch für die Managed Workplaces und diverse andere schützenswerte Objekte.

«Sophia» kann als Sammelbecken für Sicherheitsinformationen angesehen werden. Zudem stellt es ein Inventar zur Verfügung, das von verschiedensten Quellen zusammengetragen und konsolidiert wird. Damit bietet es einen nicht zu unterschätzenden Nutzen, denn nur mit einem korrekten Inventar kann auch die IT-Landschaft sauber abgedeckt und somit das Business hinsichtlich Sicherheit dargestellt werden. Das integrierte Exception Management bietet die Möglichkeit, Abweichungen in verschiedensten Bereich abzufangen und dies auch transparent auszuweisen. Durch die Anbindung von verschiedenen externen Security-Informationsprovidern (z. B. Schwachstellenbulletins) erhält «Sophia» zusätzlichen Gehalt, der dann auch in die Reports einfliesst.

Für «Sophia» werden Techniken wie Big Data oder REST-API-Schnittstellen genutzt und zur Verfügung gestellt. Ein mandantenfähiges Webportal bietet letztlich die Schnittstelle zum Sicherheitsverantwortlichen, der dort die Maturität der Security detailliert und in Echtzeit überwachen kann.

Bild 14: Mit dem Webportal von «Sophia» lässt sich die Maturity der Sicherheit in Echtzeit überwachen (Screenshot zeigt keine reale Auswertung).

9 Die Rolle des Staates

Selbst das raffinierteste Sicherheitskonzept und die fitteste Sicherheitsorganisation schützen nicht vor allen heute denkbaren Bedrohungen. Hier beginnt das Feld, das zu beackern Aufgabe des Staates sein sollte. Im Wesentlichen gibt es zwei Bereiche, in denen der Staat die Unternehmen unterstützen kann – speziell, wenn es um den Schutz kritischer Infrastrukturen geht. Er kann erstens Informationen liefern und zweitens technische Unterstützung in bestimmten Bereichen leisten.

Was die Informationen angeht: In der heutigen, schnelllebigen Zeit ist es illusorisch zu glauben, der Staat könne schneller agieren als die Privatwirtschaft. Meist zirkulieren Exploits und Indicators of Compromise sehr schnell und effizient durch die Computer Security Incident Response Teams dieser Welt. Diese Einrichtungen sind untereinander sehr gut vernetzt, und es ist durchaus üblich, Erkenntnisse rasch und unkompliziert zu teilen. Da Staaten diese informellen Kanäle meist fehlen, werden sie nur selten schneller sein als die Wirtschaft. Sie können höchstens sicherstellen, dass im operationellen Bereich ein einigermassen klares Lagebild zur Verfügung steht. Darüber lässt sich dann etwa nachvollziehen, wo ein ähnlicher Angriff auch gerade stattfindet und wie die Betroffenen voneinander profitieren können.

Informieren, wenn etwas im Busch ist

Der Staat hat aber Zugang zu Informationsquellen, die der Privatwirtschaft verschlossen sind. Hier kann er unterstützend wirken. Dies muss sich nicht auf unmittelbare Bedrohungen beziehen – es kann durchaus nützlich sein, wenn die Sicherheitsorganisationen schon nur erfahren, dass es Hinweise auf Bedrohungen gibt. Das hilft den Sicherheitsorganisationen von Unternehmen dabei, sich zum Risiko-Management erste Gedanken zu machen.

«Was wäre, wenn?» – diese Frage müssen sich Unternehmen sowieso dauernd stellen. Wenn sie dies bereits auf der Basis potenzieller Bedrohungen tun können, dann sind sie im Ernstfall darauf vorbereitet. Solche Szenarien können auch gut als Basis für Übungen im Krisenstab herangezogen werden.

Damit der gewünschte Austausch funktioniert, müssen beide Seiten jedoch lernen, dass solche Informationen nicht präzise zu sein brauchen. Selbst wenn vier von fünf solcher Szenarien nie eintreten – beim fünften hat man dann einen entscheidenden Vorsprung, und die Überlegungen zu den anderen vier waren damit nicht vergeblich.

Der zweite Aspekt hinsichtlich der Rolle des Staates ist die Lieferkette. Heute muss davon ausgegangen werden, dass auch diese nicht immer vertrauenswürdig ist. Für Unternehmen ist es jedoch fast unmöglich, gelieferte Produkte auf eingebaute Hintertürchen zu testen. Einige Hersteller verbieten – zum Schutz ihres geistigen Eigentums – ein Reverse Engineering. Deshalb begibt sich ein Kunde dieser Hersteller auf sehr dünnes Eis, sollte er nach Hintertüren suchen. Es nicht zu tun, ist aber auch keine Option, besonders bei kritischen Komponenten.

Kritische Komponenten auf Hintertüren prüfen

Genau hier könnte der Staat ansetzen: Er sollte eigentlich in der Lage sein, Komponenten, die zentral für die kritische Infrastruktur sind, detailliert zu prüfen und nach Hintertüren zu suchen. Unter Umständen wäre es auch interessant, diese Resultate zu veröffentlichen und damit die Botschaft in die Welt zu schicken: «Wir schauen genau hin.»

Neben all dem hat der Staat selbstverständlich auch eine steuernde Rolle. Er muss daran interessiert sein, dass speziell die Betreiber kritischer Infrastrukturen ihren Aufgaben nachkommen. In der Schweiz setzt die Cyber-Security-Strategie des Bundes auf die Eigenverantwortung der Firmen. Das entspricht hierzulande der Kultur und der Art und Weise, wie man miteinander umzugehen pflegt. Aber vollständig auf die Eigenverantwortung zu setzen, wäre zu riskant. Eine gewisse Kontrolle muss und soll sein.

Hier gilt es aber aufzupassen, dass seitens der Regierungen nicht überreguliert oder falsch reguliert wird. Es gibt Beispiele, bei denen die Regulatoren vor allem im Umfeld der Incident Response die Handlungsfreiheit der Unternehmen durch Vorschriften eingeschränkt haben. Hier wurde im Sinne einer umsetzbaren Kontrolle etwa auf einfach zu messende Faktoren gesetzt. Damit gewinnt man Compliance, aber keine Sicherheit. Sinnvoll wäre, wenn die Prozesse reguliert und auditiert würden. Das hiesse, Fragen zu stellen wie: Kommt das Unternehmen der Pflicht des Risiko-Managements nach? Werden Sicherheitsrisiken konsequent erfasst und bearbeitet? Damit würde geprüft, ob eine Unternehmensleitung ihrer grundlegenden Sorgfaltspflicht auch in der IT nachkommt. Die Risiken des Business werden ja seit jeher erfasst und gepflegt.

Zusätzlich könnte auch die Breite geprüft werden, in der ein Information Security Management System wirkt. Viele Firmen arbeiten bereits nach Industrie-Frameworks wie COBIT oder ISO 27001. Letzteres ist zertifizierbar und kann problemlos von einer Regierung eingefordert werden. Es ist zwar illusorisch, davon auszugehen, dass eine ISO-27001-Zertifizierung eine flächendeckende und hochstehende Sicherheitsarbeit garantiert. Aber sie kann immerhin sicherstellen, dass alle Themen auf die eine oder andere Art angegangen werden. Dies wäre sicher ein Fortschritt im Vergleich zu heute.

Anhang

Bedrohungsradar

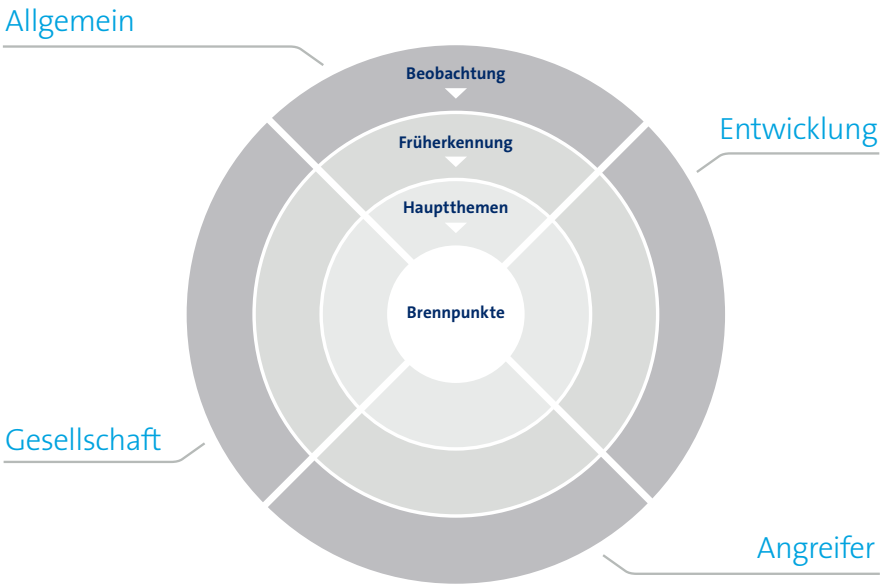


Bild 15: ***Beispiel für die Struktur eines Bedrohungsradars.***

Der Bedrohungsradar besteht aus verschiedenen Sektoren und Kreisen. Die Sektoren gruppieren die Bedrohungen und schaffen so eine gewisse Struktur. Die Kreise beschreiben die Wichtigkeit und Dringlichkeit von Bedrohungen nach folgender Hierarchie:

Beobachtung: Hier werden Bedrohungen erfasst, die in den nächsten Jahren aktuell werden könnten. Die Sicherheitsorganisation behält sie im Auge, investiert momentan aber sehr reduziert Zeit und Geld.

Frühwarnung: Solche Bedrohungen müssen im Auge behalten und eventuell Indikatoren geschaffen werden, um Bewegungen frühzeitig zu erkennen.

Hauptthemen: Bedrohungen in diesem Ring sind aktuell und müssen bearbeitet werden.

Brennpunkte: Solche Bedrohungen sind hochaktuell, ihnen gehen meist auch Ereignisse voraus.

Im Rahmen der täglichen Arbeit in der Sicherheitsorganisation werden die Bedrohungen erfasst, und anhand der Beobachtungen wird verfolgt, in welche Richtung sie sich auf dem Radar bewegen. Die Spur, die sie dabei hinterlassen, vermittelt einen Eindruck, wohin sie sich in den nächsten 12 bis 18 Monaten entwickeln könnten.

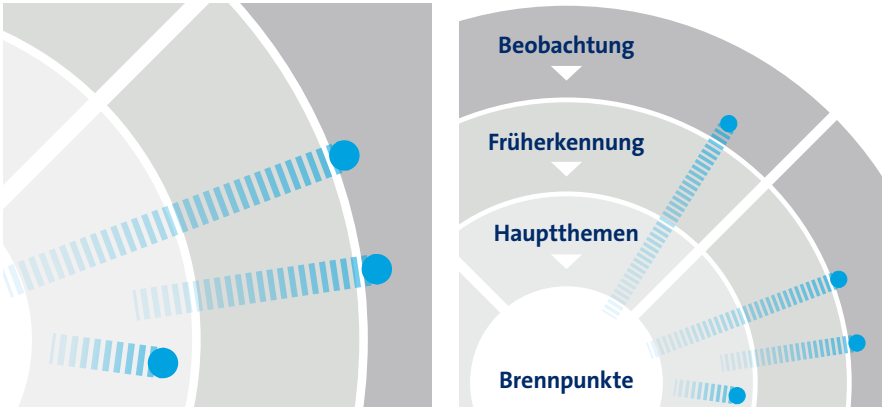


Bild 16: Die Spur, die eine Bedrohung auf dem Radar hinterlässt, zeigt, wohin sich die Bedrohung entwickeln könnte.

Abkürzungen und Fachbegriffe

APT Advanced Persistent Threat, zu Deutsch «fortgeschrittene, andauernde Bedrohung», ist ein komplexer, zielgerichteter und effektiver Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten von Unternehmen, die aufgrund ihres technischen Vorsprungs potenzielle Opfer sind. Alternativ werden auch Firmen angegriffen, die bloss als Sprungbrett zu den tatsächlichen Opfern dienen.

Architektur Bezeichnet alle statischen und dynamischen Aspekte der IT in einem Unternehmen. Hierzu zählen unter anderem die > Infrastruktur und das dazugehörige Management (Konfigurations- und Kapazitätsplanung, Lastverteilung, Datensicherung, Verfügbarkeit, Ausfallsicherheit, Katastrophenfall-Planung etc.). Darüber hinaus sind funktionale Aspekte wie die notwendigen Schnittstellen gemeint, die eine IT-Unterstützung der Prozesse ermöglichen.

Big Data Darunter werden heute in der Regel die Techniken zum Sammeln und Auswerten von wenig strukturierten Massendaten verstanden.

BYOD Bring your own Device bezeichnet das Konzept, private mobile Endgeräte in das Unternehmensnetz zu integrieren.

COBIT Control Objectives for Information and Related Technology ist ein international anerkanntes Framework zur IT-Governance. Es gliedert die Aufgaben der IT in Prozesse und Control Objectives (oft als «Kontrollziele» oder «Steuerungsvorgaben» übersetzt). COBIT definiert nicht vorrangig, wie die Anforderungen umzusetzen sind, sondern primär, was umzusetzen ist.

Continuity Management Betriebskontinuitätsmanagement bezeichnet in der Betriebswirtschaftslehre die Entwicklung von Strategien, Plänen und Handlungen, um überlebenswichtige Tätigkeiten oder Prozesse eines Unternehmens zu schützen bzw. alternative Abläufe zu ermöglichen.

CSIRT Computer Security Incident Response Team bezeichnet eine Gruppe von Sicherheitsfachleuten, die bei konkreten IT-Sicherheitsvorfällen als Koordinatoren mitwirken bzw. sich ganz allgemein mit Computersicherheit befassen, vor Sicherheitslücken warnen und Lösungsansätze anbieten, sowie Schadsoftware analysieren.

CVSS Common Vulnerability Scoring System (wörtlich übersetzt: allgemeines Verwundbarkeitsbewertungssystem) ist ein offener Industriestandard zur Bewertung des Schweregrades von möglichen oder tatsächlichen Sicherheitslücken in IT-Systemen.

Governance Unternehmensführung (Lenkungsform) bezeichnet das Steuerungs- und Regelungssystem eines Unternehmens oder Unternehmensbereichs.

IAM Identity and Access Management, in der IT meist Softwarekomponenten, die die Identitäten und deren Zugriffsrechte auf ein System verwalten.

Infrastruktur Gesamtheit aller Gebäude, Kommunikationsdienste (Netz), Maschinen und Software, die einer übergeordneten Ebene durch eine untergeordnete Ebene (lat. infra «unter») für die Informationsverarbeitung zur Verfügung gestellt werden.

ISF Information Security Forum (ISF) ist eine unabhängige Non-Profit-Organisation, deren Mitglieder sich aus grossen, internationalen Unternehmen rekrutieren. Sie befasst sich mit den Grundlagen und Konzepten für die IT-Sicherheit und stellt Werkzeuge bereit.

ISO 27001 Die Internationale Norm mit dem Subtitel «Information technology – Security techniques – Information security management systems – Requirements» spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems unter Berücksichtigung der IT-Risiken im Unternehmen.

ITSLB IT Security Level Basic ist ein Framework, das auf technischem Niveau beschreibt, wie beispielsweise ein Objekt sicher konfiguriert sein muss.

KPI Key Performance Indicator bezeichnet in der Betriebswirtschaftslehre Kennzahlen, anhand derer der Fortschritt oder der Erfüllungsgrad hinsichtlich wichtiger Zielsetzungen oder kritischer Erfolgsfaktoren einer Organisation gemessen und/oder ermittelt werden kann.

KSI In der IT-Sicherheit gebräuchliche Kennzahl, die analog zum betriebswirtschaftlichen > KPI verwendet wird.

Logging Steht in der Informatik generell für das (automatische) Speichern von Prozessdaten oder Datenänderungen. Diese werden in sogenannten Logdateien hinterlegt bzw. gespeichert.

Monitoring Überbegriff für alle Arten der unmittelbaren systematischen Erfassung (Protokollierung), Beobachtung oder Überwachung eines Vorgangs oder Prozesses mittels technischer Hilfsmittel oder anderer Beobachtungssysteme.

Policy Eine interne Leit- bzw. Richtlinie, die formal durch das Unternehmen dokumentiert und über ihr Management verantwortet wird. In der IT können Policies auch als Rahmenvorschriften für Berechtigungen und Verbote verstanden werden.

RASCI Technik zur Analyse und Darstellung von Verantwortlichkeiten in Unternehmen. Der Name leitet sich aus den Anfangsbuchstaben der englischen Begriffe Responsible, Accountable, Consulted und Informed ab.

REST Representational State Transfer ist ein Programmierparadigma für verteilte Systeme, insbesondere für Webservices und Maschine-zu-Maschine-Kommunikation.

Risiko-Management Umfasst sämtliche Massnahmen zur systematischen Erkennung, Analyse, Bewertung, Überwachung und Kontrolle von Risiken.

SIEM Security Information & Event Management ist eine Software oder ein Dienst, der Sicherheitswarnungen von Hard- und Software in einem Netzwerk in Echtzeit analysiert.

Threat In der IT-Sicherheit üblicher Begriff für Bedrohung.

Stichwortverzeichnis

Notizen

Notizen

Swisscom AG
Alte Tiefenaustrasse 6
3048 Worblaufen