Was ist Cyber Security?

2

Die wichtigsten Begriffe als Eckpfeiler eines Fachgebiets

Geleitwort: Von vermeidbaren Angriffen zu sprechen ist irreführend, weil man so davon ausgeht, dass Angreifer auf unsere Sicherheitsbemühungen nicht reagieren würden.

Sicherheitsprofis leben tagein, tagaus mit Begriffen wie Bedrohung, Risiko oder Schwachstelle. Sie denken irgendwann in Risiken und mit der Zeit geht das Wissen darüber verloren, dass man auch ein Leben führen kann, in dem man sich nicht immer wieder die Frage stellt, was bei dieser oder jener Sache alles schief gehen kann. Sicherheitsprofis verlieren so mit der Zeit das Verständnis für Menschen, die in Chancen denken und nicht in Risiken. Entscheider hingegen müssen das Berufsleben als Chance begreifen und ihr Fokus liegt darauf, die Welt als Füllhorn der Möglichkeiten zu erkennen.

In gewisser Weise stehen sich Entscheider und Security-Experten also in ihrem Begriffsverständnis gegenüber. Oder besser: Sie sind die sich gegenseitig ergänzenden Teile eines funktionierenden Ganzen. Überspitzt könnte man sagen, dass dort, wo beispielsweise der Kaufmann im Vertrieb die Märkte der Zukunft sieht, die zuständige IT-Sicherheitsbeauftragte nur zusätzliche Angriffsmuster erkennt. Chancen und Risiken stehen sich so im innerbetrieblichen Gefüge gegenüber. Die Entscheidung, welche Sichtweise bei der Ausrichtung des Unternehmens die Oberhand gewinnt, oder wie ein Ausgleich erreicht wird, müssen Geschäftsführer, Vorstände und Behördenleitungen treffen – eine klassische Führungsaufgabe also, die wenig mit Technik zu tun hat. Den Rahmen für diesen Ausgleich setzt die Politik durch Datenschutzgesetze oder das neue IT-Sicherheitsgesetz.

S. Klipper, *Cyber Security,* essentials, DOI 10.1007/978-3-658-11577-7_2

Dieses Kapitel vermittelt Ihnen die wichtigsten Begriffe der Cyber Security, die in gewisser Weise die Eckpfeiler dieses Wissensgebiets darstellen und es Ihnen ermöglichen, kompetent an aktuellen Diskussionen teilzunehmen.

2.1 IT-Sicherheit und Co

Cyber Security wird häufig synonym zu den Begriffen IT-Sicherheit und Informationssicherheit verwendet. In Fachkreisen wandelte sich der Begriff IT-Sicherheit jedoch in Richtung Informationssicherheit und in der gesellschaftlichen und politischen Diskussion gewinnt der Begriff der Cyber Security an Bedeutung, der vor wenigen Jahren noch eher ungebräuchlich war.

Das Wort Sicherheit an sich beschreibt im allgemeinen Begriffsverständnis einen Zustand, der frei von Gefahr ist. Cyber Security, IT-Sicherheit bzw. Informationssicherheit sind also Zustände, in dem der Cyber Raum, die IT bzw. Informationen frei von Gefahr sind.

Cyber Security ist gewährleistet, wenn im Cyber Raum
- Funktionssicherheit,
- Betriebssicherheit,
- Informationssicherheit,
- Datensicherheit,
- Datensicherung und
- Datenschutz gewährleistet sind.

Beim genaueren Verständnis der Begriffe im Deutschen hilft auch ein Blick auf die englische Übersetzung. Das deutsche Wort Sicherheit wird in diesem Zusammenhang im Englischen durch drei bzw. vier Begriffe repräsentiert:

- Safety
- Security
- Protection
- (Privacy)

Schauen wir uns die Bedeutung der englischen Sicherheits-Begriffe zunächst näher an, bevor wir den zentralen Begriff der Cyber Security – die Informationssicherheit – genauer betrachten:

Der englische Begriff Safety
entspricht im Deutschen der Funktionssicherheit bzw. der Betriebssicherheit. Funktionssicher heißt, dass die Ist- Funktionalität mit der Soll-Funktionalität übereinstimmt, das System also richtig funktioniert. Betriebssicher heißt kurz gesagt: Man kann sich nicht verletzen oder ähnliches. Man sollte voraussetzen, dass so etwas in der Soll-Funktionalität ausgeschlossen wurde.

Security meint im Deutschen
die Informationssicherheit. So bezeichnet man die Sicherheit in Informationssystemen, die nur solche Zustände annehmen, die zu keiner unerlaubten Informationsveränderung oder Informationsgewinnung führen. Der Informationssicherheit kommt daher unter dem Schlagwort Cyber Security eine besondere Bedeutung zu.

Protection wird im Deutschen
mit Datensicherheit und Datensicherung übersetzt. Gemeint ist die Eigenschaft eines Informationssystems, nur solche Zustände anzunehmen, die keinen unerlaubten Zugriff auf Daten und Systemressourcen erlauben. Mit Daten sind hier nicht die Daten im Sinne des Datenschutzgesetzes gemeint, sondern im Sinne der Informatik. Datensicherung bezeichnet das Anfertigen von Backups.

Der englische Begriff Privacy
entspricht im Deutschen dem Wort Datenschutz und meint den gesetzlich geregelten Datenschutz, der in verschiedenen Ländern deutliche Unterschiede aufweist.

Bildlich gesprochen nimmt der Begriff Security die zentrale Position ein, wird durch Safety und Protection flankiert und durch Privacy ergänzt. Der zentrale Begriff Security – oder in unserem Zusammenhang auch Informationssicherheit – wird durch die Aufzählung zu erreichender Schutzziele definiert, die im nächsten Abschnitt genauer beschrieben werden:

Informationssicherheit ist gewährleistet, wenn die Schutzziele
- Vertraulichkeit,
- Integrität und
- Verfügbarkeit sichergestellt sind und darüber hinaus auch
- Authentizität,
- Zurechenbarkeit,
- Nichtabstreitbarkeit und
- Verlässlichkeit gewährleistet sind.

2.2 Schutzziele

Den Schutzzielen kommt in der Begriffswelt der Cyber Security eine zentrale Bedeutung zu.

Die Vertraulichkeit (englisch: confidentiality)
eines Systems schließt eine unerlaubte Informationsgewinnung aus. Vertraulichkeit ist die Eigenschaft einer Information, niemals einem unberechtigten Individuum, einer Entität oder einem Prozess gegenüber verfügbar gemacht oder offengelegt zu werden. Vertraulichkeit beschränkt die Verfügbarkeit. Verletzungen der Vertraulichkeit werden in der Öffentlichkeit am ehesten als Vorfall und als Bruch der Cyber Security wahrgenommen.

Beispiel

Bei den Enthüllungen von Edward Snowden handelt es sich um eine Verletzung der Vertraulichkeit. Die Vertraulichkeit wäre aber auch schon verletzt, wenn vertrauliche Daten unberechtigt auf einen externen Datenträger überspielt wurden, ohne dass sie schon einer unberechtigten Person zur Kenntnis gelangt sind. Entscheidend ist, dass die Informationen sich nicht mehr dort befinden, wo sie hingehören, oder sie dort nicht mehr vor unberechtigtem Zugriff geschützt sind.

Integrität (englisch: integrity)
steht für die Manipulationssicherheit eines Systems und schließt die unerlaubte und unbemerkte Veränderung aus. Integrität ist die Eigenschaft, richtig und vollständig zu sein.

In der öffentlichen Wahrnehmung wird selten an Integritätsverletzungen gedacht, wenn es um Verletzungen der Cyber Security geht. Dass dies unberechtigt ist, zeigt das folgende Beispiel. Es macht auch deutlich, dass Angreifer längst nicht mehr nur die Technik angreifen. Sie wollen gezielt das Top-Management, unternehmerische Entscheidungen, Investments und Börsengeschäfte beeinflussen – also typische Betrachtungsgegenstände der Wirtschaftswissenschaften. Das folgende Beispiel macht auch klar, dass auf der Angreiferseite fortgeschrittenes wirtschaftswissenschaftliches Know-how vorliegt. Das Technische Know-how ist der unkomplizierteste Teil des folgenden Angriffs:

Beispiel

Im November 2014 wurde bekannt [1], dass die Hackergruppe FIN4 hunderte Beraterfirmen, Anwälte, Unternehmen und Investoren der Pharma-Branche über Monate ins Visier genommen hatte, um durch Insiderwissen von Kurs-

schwankungen profitieren zu können. Die Gruppe hatte gezielt das Top-Management angegriffen und sich dabei auf die Unternehmensbereiche Recht, Risiko und Regulatory Compliance konzentriert. Wer hier Insiderwissen hat, kann an der Börse mit seinem Wissensvorsprung große Gewinne erwirtschaften. Bei dem Angriff wurde aber nicht nur die Vertraulichkeit verletzt, sondern auch die Integrität der Daten. Es wurden nicht nur Daten gestohlen, sondern auch erfolgreich innerhalb der Unternehmen manipuliert, um unternehmerische Entscheidungen auf Grundlage gefälschter Daten herbeizuführen.

Verfügbarkeit (englisch: availability)
eines Systems oder Teilsystems ist gewährleistet, wenn deren berechtigte Nutzung nicht unerlaubt beeinträchtigt werden kann. Verfügbarkeit ist die Eigenschaft, auf Verlangen einer berechtigten Entität zugänglich und nutzbar zu sein.

Bei Verletzungen der Verfügbarkeit denken die meisten an Systemausfälle oder an sog. DDoS-Attacken, bei denen eine Webseite gezielt überlastet wird, damit sie für reguläre Nutzer nicht mehr erreichbar ist. So als würde ein Discounter Leute beauftragen, sich mit leerem Einkaufswagen in die Kassenschlangen bei Konkurrenten zu stellen, so dass reguläre Kunden sich abwenden, weil ihnen das Warten zu lange dauert. Das Discounter-Beispiel ist weniger weit hergeholt, als Sie vielleicht glauben:

Beispiel

Die Betreiber der Lieferdienst-Portale pizza.de und lieferando.de waren jahrelang Opfer solcher DDoS Angriffe. Zwischenzeitlich war eine Belohnung von 100.000 € auf die Ergreifung der Täter ausgesetzt. Konkurrenten gerieten schließlich als Auftraggeber für die Angriffe ins Visier der Ermittler. Im Januar 2013 wurden wegen Datenbankdiebstahls sieben Strafbefehle gegen Führungskräfte des Konkurrenten Lieferheld verhängt [2]. Im August 2014 wurde Pizza.de vom Konkurrenten Lieferheld geschluckt [3].

Auch dieses drastische Beispiel der aktuellen Vergangenheit zeigt – ebenso wie die bereits erwähnten Angriffe auf Sony – dass Verletzungen der Cyber Security sich längst nicht mehr nur im Serverraum bemerkbar machen. Cyber Security ist eng mit dem unternehmerischen Überleben verbunden und daher von entscheidender Wichtigkeit für alle Entscheider aus Wirtschaft und Politik.

Der Kern: Vertraulichkeit, Integrität und Verfügbarkeit
Die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit bilden den Kern der Informationssicherheit und sind eigentlich als abschließende Aufzählung gedacht.

Es existieren jedoch einzelne Facetten der Informationssicherheit, zu denen es weitere Schutzziele gibt, die jeweils auf einen ganz konkreten Anwendungsfall abzielen. Dies sind:

- Authentizität
- Zurechenbarkeit
- Nichtabstreitbarkeit
- Verlässlichkeit

Authentizität (englisch: authenticity)
meint die Echtheit und Glaubwürdigkeit eines Objekts. Dass sich diese Echtheit auch mit charakteristischen Eigenschaften überprüfen lässt, ist der für die Cyber Security entscheidende Punkt der Authentizität, der sich technisch und organisatorisch nicht so einfach realisieren lässt.

Beispiel

Erinnern wir uns an einen der größten Skandale der deutschen Pressegeschichte, an die Affäre um die gefälschten Hitler-Tagebücher und stellen wir uns vor, die Tagebücher seien – wie in der heutigen Zeit – elektronisch erstellt worden. Wie hätte da die Echtheit überprüft werden sollen?

Da Authentizität ein Teil der Integrität ist, passt hier auch das zuvor genannte Beispiel um Insidergeschäfte und Manipulation von Entscheidern aus der Pharma-Branche. Betroffene Manager hatten hier auf Basis gefälschter Informationen Entscheidungen getroffen.

Verbindlichkeit bzw. Nichtabstreitbarkeit (englisch: non repudiation)
liegt vor, wenn innerhalb des Informationssystems Aktionen im Nachhinein eindeutig zuzuordnen sind und nicht abgestritten werden können. Verbindlichkeit ist ein Teil der Authentizität und damit auch ein Teil der Integrität.

Beispiel

Das perfekte Beispiel wären hier bloßgestellte Dokumente eines Geheimdienstes. Hätte es sich bei den Dokumenten von Edward Snowden nur um wenige Dateien gehandelt, hätte der US Geheimdienst NSA die Echtheit (Authentizität) der Dokumente abstreiten können. Die Nichtabstreitbarkeit der Dokumente ergab sich in diesem Fall nur durch die schiere Anzahl an Dokumenten, die eine Fälschung aller Dokumente nahezu ausschließen. Die Beweiskraft einzelner

der veröffentlichten Dokumente oder einzelner darin enthaltener Aussagen ist allerdings nicht sehr hoch, weshalb sie auch für Strafverfahren schwer zu verwenden sind. Details könnten jederzeit abgestritten werden. Hinzu kommt, dass die NSA nicht genau weiß, welche Daten Edward Snowden entwendet hat und welche Beweise er noch in der Hinterhand hält. Erst die Gesamtlast der bloßgestellten Dokumente führt hier zum sehr hohen Maß an Nichtabstreitbarkeit, die von der NSA so sicher nicht beabsichtigt war.

Zurechenbarkeit (englisch: accountability)
in der IT erweitert die Nichtabstreitbarkeit von Informationen auch auf Handlungen und Ereignisse, die eine eindeutige persönliche Zurechenbarkeit gewährleistet. Es geht also zum Beispiel nicht nur darum, ob eine bestimmte Datei echt ist und nicht abgestritten werden kann, sondern auch darum, festzustellen, wer sie in ein bestimmtes Verzeichnis gelegt hat.

Beispiel

Ein Beispiel sind hier elektronisch verkaufte Dokumente von denen nicht nur die Echtheit und die Nichtabstreitbarkeit seitens des Herausgebers interessieren, sondern auch die Zurechenbarkeit zu einem bestimmten Käufer, der die Datei nicht weitergeben darf. Taucht irgendwann eine Raubkopie auf, möchte der Herausgeber wissen, welcher Kunde sie unerlaubt weitergegeben hat. Ähnliches gilt für Insider-Infos an die Presse, von denen betroffene Unternehmen gerne wissen möchten, welche Personen sie weiter geleitet haben.

Anonymität
hat sich in letzter Zeit durch die gehäuften Datenschutzskandale zu einem neuen Schutzziel entwickelt, das bisher nur selten in einer Auflistung genannt wird, dem allerdings zukünftig eine größere Bedeutung zukommen wird. Diese Einschätzung beruht auf der Erkenntnis, dass sich Daten auf Dauer nur sehr schwer schützen lassen. Daher wird die Forderung nach Anonymität immer lauter. Das liegt daran, dass der persönliche Schaden für eine betroffene Person häufig größer sein kann, als der jeweils entsprechende Teil des Schadens für eine betroffene Organisation. Zu dem Schaden der Organisation kommt so, auf Grund fehlender Anonymität, die Summe der Schäden einzelner Betroffener hinzu.

Beispiel

Im Dezember 2014 wurde eine Gehaltsliste von 30.000 Mitarbeitern des Beratungsunternehmens Deloitte veröffentlicht, die zu den größten Beratungsfirmen der Welt gehört [4]. Die Veröffentlichung der Gehälter der Mitarbeiter ist für ein Unternehmen sicher ärgerlich. Für Mitarbeiter, die auf der Suche nach einem neuen, besser bezahlten Job sind, kann das die Chancen bei einer Gehaltsverhandlung mit einem neuen Arbeitgeber stark einschränken. Auch firmenintern steht der Eine durch größere Gehaltsunterschiede plötzlich als Gewinner und der Andere als Verlierer da. Oder stellen Sie sich vor, welche Auswirkungen das auch im privaten Umfeld haben kann, wenn plötzlich jeder weiß, was man verdient.

2.3 Werte

Nach der Erläuterung der Schutzziele beschäftigen wir uns nun mit den Werten (englisch: assets) einer Organisation, auf die sich die Schutzziele ausrichten. So wird alles bezeichnet, was für eine Organisation einen Wert hat. Hierzu gehören zum Beispiel Bankdaten, geistiges Eigentum, Mitarbeiterdaten, oder Daten von Kunden, aber auch Gebäude können Werte im Sinne der Cyber Security sein, wenn beispielsweise bereits die Kenntnis des Gebäudegrundrisses oder die Anordnung der Räume geheimhaltungsbedürftig ist. Hinzu kommen alle IT-Systeme und vielfach auch deren Funktionsweise, wenn diese speziell in dieser Organisation entwickelt wurde. Denken Sie an die Algorithmen im algorithmischen Handel oder im High-Frequency Trading, bei dem es sich um einen mit Computern betriebenen Handel mit Wertpapieren handelt. Die verfolgte Anlagestrategie ist im programmierten Algorithmus enthalten.

Zu den wichtigsten Werten der Cyber Security gehören

- Informationen, Geistiges Eigentum, Geschäftsgeheimnisse, Know-how
- IT-Systeme, Software und Netzwerke
- Mitarbeiter- und Kundendaten
- Interne Betriebsabläufe und Prozess-Know-how
- Mitarbeiter und Geschäftskontakte
- Betriebsanlagen
- Gebäude, Räume
- …

2.4 Bedrohung

Bildlich gesprochen stehen die Werte einer Organisation auf der einen Seite und eine oder mehrere Bedrohungen auf der anderen. Dazwischen stehen die bereits besprochenen Schutzziele. Einerseits definieren sie, was besonders Schützenswert ist, andererseits beschreiben sie auch, wo sich ein Angriff besonders lohnen könnte.

► Schutzziele aus Sicht der Verteidiger werden aus Sicht des Angreifers zu Angriffszielen.

Aus diesem einfachen Zusammenhang ergibt sich schließlich eine Bedrohung (englisch: threat). Eine Bedrohung der Schutzziele Vertraulichkeit, Verfügbarkeit oder Integrität.

► Alles was schützenswert ist, ist angriffswürdig und umgekehrt.

Eine Bedrohung wird dadurch wiederum gleichzeitig eine potentielle Ursache für einen unerwünschten Vorfall, der negative Auswirkungen auf ein System oder die Organisation haben kann. Bedrohungen der Cyber Security gehen daher nicht nur auf Angreifer zurück.

Die Cyber Security ist auch von Naturereignissen, technischen Defekten oder Stromausfällen bedroht. Das gilt in neuerer Zeit umso mehr, da Kritische Infrastrukturen wie Stromversorger in ihrer Leistungserbringung ebenfalls von Cyberangriffen bedroht sind und ihre Kunden somit Opfer von Kolateralschäden werden können.

Der Begriff der Bedrohung wird teilweise unterschiedlich verwendet. Die folgende Aufzählung orientiert sich an internationalen Standards [5]:

Man unterscheidet Bedrohungen durch
- vorsätzliche Handlungen (deliberate) gegen Informationen und Werte,
- durch menschliche Handlungen und fahrlässig verursachte Vorfälle (accidental) und durch
- Umwelteinflüsse (environmental).

Hieraus resultieren verschiedenste konkrete Bedrohungen, die jeweils eine Klasse von Szenarien bzw. Schadensereignissen hervorbringen, zwei Begriffe, mit denen wir uns im folgenden Abschnitt befassen. Der Begriff Bedrohung ist daher etwas

schwerer zu fassen als die anderen, weil es sich bei ihm um ein substantiviertes Verb handelt. Der Begriff wird also eigentlich nicht als Subjekt oder Objekt verwendet, sondern als Prädikat:

„Die Cyber Security wird bedroht durch…“

Bedrohungen stehen also meist nicht allein als Subjekt oder Objekt. Bedrohungen drücken eine Relation zwischen Subjekt und Objekt aus, was sich sprachlich dadurch zum Ausdruck bringt, dass häufig von „Bedrohung durch etwas“ gesprochen wird. Diese Relationen werden im Rahmen einer Bedrohungsanalyse festgestellt.

Das bedeutet, dass es keine abgeschlossene Menge an Bedrohungen gibt, gegen die man sich wappnen muss. Die Menge der Bedrohungen ist für jede Organisation unterschiedlich und sie wird von den relevanten Subjekten und Objekten bestimmt und den auf ihnen möglichen Relationen. Daher sind komplexe IT-Architekturen auch bedrohter als weniger komplexe, weil die größere Anzahl an Subjekten/Objekten eine größere Anzahl von Bedrohungen zulässt.

Warum geht dieser Abschnitt so intensiv auf diese sprachlichen Spitzfindigkeiten ein? Die bisher betrachteten Begriffe der Schutzziele waren abstrakt. Auch der Begriff der Werte war relativ leicht zu fassen, während der Begriff der Bedrohung zum größten Teil auf Experteneinschätzungen beruht und daher in einigen der folgenden Überlegungen von zentraler Bedeutung sein wird. Darüber, ob eine Bedrohung relevant ist, lässt sich selbst in Expertenkreisen trefflich streiten.

Hintergrund: Advanced Persistent Threats

Der relativ junge Begriff Advanced Persistent Threats findet sich immer häufiger in den Medien. Er beschreibt eigentlich keine Bedrohung (Threat). Gemeint sind hiermit sehr gezielte, länger andauernde, unentdeckte Angriffe, die sich unter teils großem Aufwand gegen wenige Opfer richten. Meistens werden Advanced Persistent Threats mit Staaten als Angreifer oder Drahtzieher in Verbindung gebracht und richten sich gegen Behörden, Kritische Infrastrukturen, große Unternehmen oder Hidden Champions.

Als Threat (Bedrohung) werden sie bezeichnet, weil es aus unterschiedlichen technischen Gründen nahezu unmöglich ist, derartige gezielte Angriffe dauerhaft zu verhindern. Die Bedrohung ist also nicht der Angriff an sich, sondern dessen dauerhaftes Fortbestehen, also die Nicht-Entdeckung durch das Opfer. Der eigentliche Schaden wird unter Umständen erst lange nach dem Beginn des Angriffs angerichtet.

Am Beispiel der Advanced Persistent Threats zeigt sich sprachlich, dass an der einen oder anderen Ecke der Cyber Security bereits die Verteidigungslinien einbrechen und sich der Angreifer unbemerkt hinter feindlichen Linien aufhalten kann, möglicherweise ohne zunächst Schaden anzurichten. Die klassische Perimeter-Sicherung, also die Sicherung der Grenzen des Unternehmens zum Beispiel mit Firewalls hat hier ausgedient. Die Bedrohung ist nicht der Grenzübertritt an sich, wie das bei regulären Kräften der Fall wäre. Die Bedrohung ist, dass sich der Angreifer über längere Zeit unbemerkt hinter feindlichen Linien aufhalten kann.

2.5 Schwachstelle

Ausgehend vom Begriff der Bedrohung könnte man nun sagen, dass diese auf dem schützenden Dach der Cyber Security lasten. Wohl dem, dessen Dach keine „schwache Stelle“ hat, die sich als Architekturfehler entpuppen könnte.

Häufig werden Schwachstellen (engl.: vulnerabilities) in sicherheitskritischen Systemen als Fehler bezeichnet. Das ist nur bedingt richtig, denn viele Schwachstellen sind keine Fehler, sondern durchaus gewollt oder zumindest begründet und nicht zu vermeiden. So ist der Vorsprung eines Hausdachs bei Wind sicher eine Schwachstelle gegenüber der Bedrohung durch Orkane. Wenn Wand und Fenster allerdings vor Regen geschützt sein sollen, kommt man ohne einen Dachvorsprung nicht aus. Der Dachvorsprung ist aus diesem Blickwinkel also kein Fehler, sondern eine gewollte Eigenschaft.

- Eine Schwachstelle bezüglich eines Werts, ist eine gewollte oder ungewollte Eigenschaft, die einer Bedrohung ausgesetzt ist und ein Schadensereignis ermöglicht.

- Der Schutz der einen Schwachstelle kann schnell zur neuen Schwachstelle werden.

Während technisch begeisterte Hacker in der Vergangenheit ihr Augenmerk hauptsächlich auf Schwachstellen durch Fehler legten, spielt das bei heutigen Angreifern keine so zentrale Rolle mehr. Ein professioneller Angreifer versucht nicht durch aufwändige statische Berechnungen den Konstruktionsfehler im Dach zu finden, er nimmt einfach ein paar Ziegel ab und die Isolierung beiseite oder steigt wie der Weihnachtsmann durch den Kamin. In der Vergangenheit ging es um die Begeisterung an technischen Analysen und Zusammenhängen. Heute geht es darum, ein Angriffsobjekt zu kompromittieren – technisch anspruchsvoll oder nicht, ist dabei zweitrangig.

► Nicht die Suche, Analyse und Veröffentlichung der Schwachstelle treibt heutige Angreifer an, sondern die Suche der Schwachstelle, deren Ausnutzung und deren Geheimhaltung.

Noch vor wenigen Jahren war die Veröffentlichung der Schwachstelle das Ziel eines Hackers. So konnte man sein Renommee steigern und zur Beseitigung der Schwachstelle beitragen. Ein Angreifer von heute hat keinerlei Interesse daran, dass eine entdeckte Schwachstelle geschlossen wird. Im Gegenteil: Er möchte die Schwachstelle möglichst lange und exklusiv ausnutzen.

Diese Tendenz hatten wir bereits bei den Advanced Persistant Threats (APT) angesprochen, bei denen zusätzlich die ausgenutzte Schwachstelle nicht primär diejenige Schwachstelle ist, die den Grenzübertritt ermöglicht hat, sondern die, die den erfolgten Grenzübertritt dauerhaft unbemerkt lässt.

2.6 Schaden(sereignis)/Vorfälle/Szenarien

Ein Schaden (engl.: impact) bezeichnet die Auswirkung auf die erreichte Höhe der Unternehmensziele. Diese können materiell und immateriell sein. Der Sachverhalt, der zu einem Schaden führt, wird auch als Schadensereignis bezeichnet. Ein oder mehrere Ereignisse bilden einen Vorfall.

► Ein oder mehrere Ereignisse, die einen Schaden verursachen, werden als Vorfall bezeichnet.

Ausgehend von vergangenen Vorfällen und theoretischen Überlegungen für denkbare Schadensereignisse können Szenarien entwickelt werden, anhand derer man die Verwundbarkeit der Cyber Security berücksichtigen kann.

► Szenarien bestehen aus denkbaren Schadensereignissen.

Ein Cyber Security Vorfall besteht also aus einem oder mehreren unerwünschten oder unvorhergesehenen Sicherheitsereignissen, die mit einer hohen Wahrscheinlichkeit eine Beeinträchtigung der Geschäftstätigkeit bedeuten und die Cyber Security bedrohen.

Mit dieser Feststellung kommen wir zum eigentlichen Schlüsselbegriff, der verdeckt oder offen bei nahezu allen Diskussionen zum Thema Cyber Security eine wichtige Rolle spielt: die Wahrscheinlichkeit.

2.7 Wahrscheinlichkeit

Wahrscheinlichkeiten sind ein zentraler Betrachtungsgegenstand aller Bemühungen zur Cyber Security, der vielerlei Schwierigkeiten mit sich bringt. Beginnen wir mit der kleinsten Schwierigkeit – der Frage, was eine hohe, mittlere oder geringe Wahrscheinlichkeit ist. Wir kommen so zu einem zentralen Problem, dass allen Diskussionen zu Sicherheitsthemen in Unternehmen und Behörden innewohnt.

Sie hatten mit diesem Problem vielleicht schon im Rahmen der Stochastik zu tun und erinnern sich eventuell an die Probleme, die entstehen, wenn man aus einer Kardinalskala mit diskreten Werten plötzlich eine Ordinalskala macht: Auf einer Ordinalskala sind nicht die gleichen mathematischen Rechenoperationen möglich. Man kann also nicht zwei „mittlere" Wahrscheinlichkeiten addieren. Will man mit der in einer Ordinalskala (zum Beispiel gering, mittel und hoch) angegebenen Wahrscheinlichkeit rechnen, muss man sie wieder in eine Kardinalskala überführen. Hierfür bietet sich jeweils die „Mitte" der Werte an – oder deren Grenzen. Die Ordinalskala gering, mittel, hoch kann auf drei oder fünf diskrete Werte abgebildet werden, mit entsprechenden Auswirkungen. Bei drei Werten gibt es keine 100-prozentige Wahrscheinlichkeit und keine Ereignisse die unwahrscheinlich sind und bei fünf Werten stehen die mittleren drei Werte nur für zwei der ursprünglichen Skalenwerte. Will man mit diesen Zahlen rechnen – und das will man – kommt es entsprechend der Abbildungsvorschrift teils zu erheblich unterschiedlichen Ergebnissen. Insbesondere auch deshalb, weil die diskreten Werte rein willkürlich festgelegt werden können, dass heißt, die Werte gering, mittel und hoch müssen nicht proportional zueinander sein.

► In der Security genutzte Wahrscheinlichkeiten unterliegen aufgrund der genutzten Skalen teils großen Verzerrungen bezüglich einer Gesamtbetrachtung.

Beispiel

Ein Security-Experte führt eine Expertenbefragung zur Eintrittswahrscheinlichkeit unterschiedlicher Schadensereignisse durch. In der Befragung stellt er Wahrscheinlichkeiten in Prozent zur Auswahl: 0 %, 10 %, 20 % etc. Er fragt: „Wie hoch ist die Wahrscheinlichkeit, dass dieses Schadensereignis im nächsten Jahr eintritt?" Danach ordnet er die Durchschnittsergebnisse der Befragung der unternehmensinternen Wahrscheinlichkeits-Skala zu: gering (0 % bis < 50 %), mittel (> 50 % bis < 75 %) und hoch (> 75 % bis 100 %). Hierbei fallen Scha-

densereignisse mit 0 % Wahrscheinlichkeit in die gleiche Kategorie wie die mit 49 % Wahrscheinlichkeit. Und was ist mit Schadensereignissen, die im nächsten Jahr zwei Mal eintreten? Diese Fragen sind nicht weiter von Bedeutung, wenn es zum Beispiel nur darum geht, die Schadensereignisse mit mittlerer und hoher Wahrscheinlichkeit zu ermitteln und zu unterscheiden. Häufig wurden die Skalen genau dazu entwickelt. Will man später allerdings wissen, ob drei gering wahrscheinliche Schadensereignisse drängender sind als ein mittel wahrscheinliches, gerät man in der Ordinalskala an seine Grenzen und muss wieder zurück zu den Ursprungswerten, die dann häufig nicht mehr verfügbar sind.

Vielleicht stellen Sie sich jetzt die Frage, warum das trotz der mitunter großen Auswirkungen die kleinste Schwierigkeit mit den Wahrscheinlichkeiten von Schadensereignissen sein soll. Das liegt daran, dass es einfach ist, sie zu beschreiben, zu analysieren und mit ihr umzugehen. Bei der nächsten Schwierigkeit ist das nicht mehr der Fall.

- Wahrscheinlichkeiten sind Schätzgrößen oder Erfahrungswerte der Vergangenheit mit begrenzter Aussagekraft für die Zukunft.

- Dies gilt umso mehr in der sich ständig ändernden IT-Landschaft von Unternehmen und Behörden.

Zu Wahrscheinlichkeiten kann man daher auch unterschiedlichster Meinung sein, weil keiner von uns in die Zukunft sehen kann. So schlimm es sich auch anhört: Das einzige was man erreichen kann, ist die Trefferquote beim Raten zu erhöhen. Selbst wenn für ein Szenario belastbare statistische Daten vorliegen, sind diese für kleine und mittlere Unternehmen nur bedingt anzuwenden.

Vor allem lassen sich Szenarien nicht so ohne weiteres von einem auf das andere Unternehmen oder von der Vergangenheit in die Zukunft übertragen. Gehen wir von einer geschätzten zukünftigen Eintrittswahrscheinlichkeit eines Schadensereignisses aus, dass sich vor drei Jahren bei einem anderen Unternehmen ereignet hat. Dies stellt oftmals keine gesicherte Entscheidungsgrundlage für oder gegen eine Sicherheitsmaßnahme dar, die auch am Ende eines zehn Jahre laufenden Outsourcing-Vertrags noch hilfreich sein soll. Dieser Sachverhalt ist einer der Kernpunkte aktueller Sicherheitsprobleme großer Organisationen mit unzureichenden Sicherheitsvorkehrungen, die auf Wahrscheinlichkeiten basieren, die sich teils auf lange zurückliegenden Schadensszenarien beziehen.

2.8 Schadenshöhe

Der Begriff der Schadenshöhe wurde bisher nicht explizit erwähnt, er unterliegt aber leider ähnlichen Verwerfungen wie die Wahrscheinlichkeit.

- Schadenshöhen sind ebenso wie Wahrscheinlichkeiten Schätzgrößen oder Erfahrungswerte der Vergangenheit mit begrenzter Aussagekraft für die Zukunft.

- Dies gilt umso mehr in der sich ständig ändernden IT-Landschaft von Organisationen und vor dem Hintergrund ständig wechselnder Angriffsszenarien.

Beispiel

Ein unbekannter Hacker dringt in ein Unternehmen ein und stiehlt höchst vertrauliche Konstruktionsdaten. Wie hoch der Schaden dieses Ereignisses ist, kann eventuell erst Jahre später ermittelt werden. Es kann sein, es war ein technikbegeisterter Hacker alter Schule, bei dem die Daten nun besser aufgehoben sind, als im eigenen Unternehmen. Es kann aber auch sein, es war ein Geheimdienst, der gar nicht gefunden hat, was er gesucht hat und alles wieder vernichtet, oder es kann sein, dass es ein Auftragshack der Konkurrenz war. Selbst wenn man drei oder fünf Jahre später eine eventuelle Schadenshöhe ermittelt hat, lassen sich die Ergebnisse nur äußerst beschränkt auf die Zukunft übertragen.

Das Beispiel zeigt, wie schwer es ist, aus der Vergangenheit in die Zukunft zu schauen. Märkte ändern sich, Unternehmen wachsen, verschwinden oder werden verkauft und Angreifer wechseln ihre Motive. Darüber hinaus werden Schadenshöhen einzelner Szenarien oder Ereignisse in der Cyber Security ebenfalls häufig in Ordinalskalen erfasst (zum Beispiel gering, mittel und hoch) und unterliegen damit einer skalenbedingten Unsicherheit, wie wir sie bereits bei den Wahrscheinlichkeiten kennengelernt haben.

- In der Cyber Security genutzte Schadenshöhen unterliegen ebenso wie Wahrscheinlichkeiten aufgrund der genutzten Skalen teils großen Verzerrungen.

2.9 Risiko

Kapitel 2 wurde mit einem Zitat von Giovanni Agnelli eingeleitet: „Es ist unmöglich, ein unnötiges Risiko einzugehen. Denn ob das Risiko unnötig war, findet man erst heraus, wenn man es längst eingegangen ist." In der Cyber Security bezeichnet man als Risiko Unsicherheiten bei der Erreichung der Ziele der Organisation, die sich aus der Nutzung des Cyber Raums ergeben. Dabei wird das Risiko als Produkt aus Wahrscheinlichkeit und Schadenshöhe eines Ereignisses dargestellt. Sie ahnen sicher schon, zu welcher wichtigen Feststellung uns das führt:

- Risiken basieren auf Schätzgrößen oder bisherigen Erfahrungswerten zu Wahrscheinlichkeiten und Schadenshöhen mit begrenzter Aussagekraft für die Zukunft. Ihre Einschätzung unterliegt dadurch einer größeren Unsicherheit als die Ausgangswerte.

In der Cyber Security ermittelte Risiken werden ebenso wie Wahrscheinlichkeiten und Schadenshöhen zunächst als diskrete Größen ermittelt und dann in Ordinalskalen übertragen (zum Beispiel gering, mittel und hoch). Hierdurch werden die sich multiplizierenden Unsicherheiten bei Wahrscheinlichkeiten und Schadenshöhen ein weiteres Mal verstärkt.

- In der Cyber Security genutzte Risikoeinschätzungen unterliegen aufgrund unsicherer Grundlagen und der genutzten Skalen teils immensen rechnerisch möglichen Verzerrungen.

Beispiel

Ich habe in meiner eigenen Beratungspraxis einen Fall erlebt, in dem das rechnerisch zu ermittelnde jährliche Gesamtrisiko aus dem Risikoinventar je nach Interpretation und Festlegung der Skalen um den Faktor 20 voneinander abwich. Als Rechenbeispiel zur Verdeutlichung: 5 Mio. oder 100 Mio. – 50 Mio. und über einer Milliarde? Das Rechnen mit konkreten Zahlen ist in diesen Fällen meist nur sehr selten möglich, weil in der Dokumentation oft nur die groben Ordinalskalen genutzt wurden.

Als Wirtschaftswissenschaftler erkennt man sofort die dahinter stehende Brisanz. Für derartige Risiken sind unter Umständen Rückstellungen zu bilden, die nicht unerheblich sind und durchaus auch mal ein schwaches Jahresergebnis ins Negative kippen können. Dies ist vor allem vor dem Hintergrund brisant, dass die

wenigsten Unternehmen bisher ein aussagekräftiges IT-Risikoinventar besitzen. Selbst wenn, fußen diese nicht auf systematischen Assessments, sondern entstehen meist „auf Zuruf" und standardkonforme Information Security Risk Management Systeme, die in das unternehmensweite Risikomanagement eingebunden sind, stecken in den Kinderschuhen.

Nicht, dass die bisherigen Rechengrößen bereits unsicher genug seien. In den meisten Unternehmen werden die genutzten Ordinalskalen für die Dokumentation möglicher Schadenshöhen ebenfalls voneinander abweichen.

Beispiel

Ein internationales Finanzinstitut wird seine Kreditausfall- oder Währungsrisiken in einer anderen Skala beurteilen als seine Risiken aus dem Bereich Cyber Security.

Es ist durchaus anzunehmen, dass unter dem Stichwort Cyber Security Risiken in den nächsten Jahren allein durch die erstmalige Erfassung und Analyse faktisch vorhandener Risiken, große bilanzwirksame Verwerfungen auf die deutsche Wirtschaft zukommen. Wenn Security-Experten und Ökonomen hier nicht an einem Strang ziehen, kommen auf beide Seiten unschöne Zeiten zu.

2.10 Maßnahme

Die letzten Abschnitte waren dominiert von Schwierigkeiten, Unsicherheiten und Problemen. Kommen wir nun zu den Lösungen und damit zum eigentlichen Herzstück der Cyber Security – den Maßnahmen (engl.: control, measure, safeguard und countermeasure).

Maßnahmen im Bereich der Cyber Security dienen der Modifikation von Risiken. Nachdem wir uns bereits ausführlich mit den Begriffen Eintrittswahrscheinlichkeit, Schadenshöhe und Risiko auseinander gesetzt haben, können wir festhalten:

- Maßnahmen der Cyber Security modifizieren die Höhe des Risikos durch Verringerung von Eintrittswahrscheinlichkeit und/oder Schadenshöhe.

Welche Maßnahmen nun für eine Organisation richtig und wichtig sind und in welcher Reihenfolge diese umzusetzen sind, hängt direkt mit all den in den vorherigen Abschnitten behandelten Begriffen und den anhaftenden Unsicherheiten zusammen.

Welche Maßnahmen sind richtig und wichtig?

- Welche Werte möchte ich beschützen?
- Welchen Bedrohungen unterliegen die Schutzziele?
- Welche Schwachstellen könnte ein Angreifer ausnutzen?
- Zu welchen Schadensereignissen und Vorfällen könnte es kommen?
- Welche Szenarien wären denkbar?
- Mit welcher Schadenshöhe wäre dabei zu rechnen?
- Wie wahrscheinlich sind die Vorfälle und Szenarien?
- Welches Risiko ergibt sich daraus?

Wer bei der Frage der Notwendigkeit von Maßnahmen mitreden möchte, muss diese Fragen verstehen und die Bedeutung sowie die Zusammenhänge der verwendeten Schlagworte kennen – das sollte in diesem Kapitel deutlich geworden sein. Darüber hinaus ist es wichtig, zu wissen, dass die Bestimmung der Notwendigkeit von Maßnahmen teilweise hochspekulativ sein kann. Sie ist in hohem Maß von der Beurteilung vergangener Ereignisse anhand des aktuellen Stands von Forschung und Technik abhängig, aufgrund derer für die Zukunft nötige Maßnahmen festgelegt werden.

Um hier im Rahmen aller unvermeidlichen Unsicherheiten nicht vollends ins Orakeln abzurutschen, ist ein hohes Maß an Spezialisierung notwendig und die Abstützung auf anerkannte und erprobte Industriestandards und Best Practices wie die ISO/IEC 27001 oder den BSI IT-Grundschutz.

Hintergrund: Maßnahmenkatalog des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) liefert mit dem BSI IT-Grundschutz eine umfangreiche Maßnahmenempfehlung, die auf der Überlegung aufbauen, dass alle bedrohten Schwachstellen mit einer Maßnahme zu versehen sind. Die Ermittlung von zweifelhaften Wahrscheinlichkeiten entfällt so. Eine Priorisierung wird nicht über das Risiko, sondern über den Schutzbedarf ermittelt, der auf einer dreistufigen Skala normal, hoch und sehr hoch angegeben wird. Zusätzlich ist jede Maßnahme einer von vier Maturitätsstufen des Security Managements zugeordnet, so dass der Einstieg erleichtert werden soll – von der Eingangsstufe bis zum Zertifikat.

Literatur

1. FIN4: Stealing Insider Information for an Advantage in Stock Trading?, FireEye Webseite (veröffentlicht am 30.11.2014, eingesehen am 15.01.2015) https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html
2. Strafbefehle gegen Lieferdienst-Startup, Heise Online (veröffentlicht am 03.01.2013, eingesehen am 15.01.2015), http://www.heise.de/newsticker/meldung/Strafbefehle-gegen-Lieferdienst-Startup-1776645.html
3. Lieferheld schluckt Pizza.de, Heise Online (veröffentlicht am 14.08.2014, eingesehen am 15.01.2015), http://www.heise.de/newsticker/meldung/Lieferheld-schluckt-Pizza-de-2292836.html
4. Hacker veröffentlichen umfangreiche Gehaltslisten, Süddeutsche Zeitung (veröffentlicht am 04.12.2014, eingesehen am 16.01.2015), http://www.sueddeutsche.de/digital/mysterioeser-angriff-hacker-veroeffentlichten-umfangreiche-gehaltslisten-1.2251740
5. ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management (2011), International Organization for Standardization (ISO)

http://www.springer.com/978-3-658-11576-0

Cyber Security
Ein Einblick für Wirtschaftswissenschaftler
Klipper, S.
2015, IX, 47 S. 1 Abb. in Farbe., Softcover
ISBN: 978-3-658-11576-0