Hase und Igel im Cyberspace

Informationssicherheit bleibt immer ein „Infinite Game“

Standards für die Informationssicherheit wie ISO 27001 und dessen Automotive-Derivat Tisax gibt es schon seit Jahren. In Industrie und Wirtschaft werden große Anstrengungen unternommen, die Infrastruktur vor Cyberattacken zu schützen. Tatsächlich gibt es nach wie vor erhebliche Lücken und Mängel - und dafür einen Grund.

Klaus Kilvinger

Informationen sind Daten, die für jedes Unternehmen von großem Wert sind und damit ein Wirtschaftsgut, welches nicht in die Hände Unbefugter gelangen sollte und das einen angemessenen Schutz erfordert. Die primären Schutzziele für Informationen sind Vertraulichkeit, Verfügbarkeit und Integrität. Diese Ziele anzustreben, ist ein fortlaufender Prozess. Die Verbesserung der Informationssicherheit – insbesondere der Cybersicherheit – erfolgt in einem so genannten „Infinite-Game-Szenario“.

Was ist ein Infinite Game?

Im *Infinite Game* steht im Gegensatz zu den *Finite Games* weder die Anzahl der Teilnehmer, noch das Ende noch die Regeln fest, nach denen gespielt wird. Auch die Ziele sind unklar, es gibt kein Endspiel, jeder Teilnehmer definiert sein Ziel für sich selbst. Der Vorsprung eines einzelnen Spielers ist nicht von Dauer, sein Status wechselt ständig ab zwischen „den anderen voraus“ und „liegt zurück“.

In der Informationssicherheit ist das analog. Es gibt keinen Beginn und kein Ende, es gibt keine Grenzen, angefangen vom Werksgelände bis zum Homeoffice des Mitarbeiters sind keine physischen Grenzen relevant. Das bisher oft rein physische Risiko von Diebstahl bzw. die Manipulation von Daten auf Computersystemen vor Ort wird durch die Anbindung an das Internet vervielfacht. Durch die Cloud und Smart Home eröffnen sich weitere völlig neue Optionen für die Handelnden. Und der in Produktionsbetrieben vorhandene Wildwuchs mit alten Systemen ohne Netzwerkanschluss, Maschinen ohne Updatefähigkeit

bis hin zu aktuellen Maschinen, die immer online sind, macht es nicht einfacher.

Zu den Bedrohungen im Internet zählen Schadprogramme wie Computerviren, Keylogger, Trojanische Pferde, Phishing-Mails und andere Angriffe. Eine eigene Branche der Cyberkriminalität hat sich entwickelt: Manche Firmen sind spezialisiert auf Ausspähen, andere entwickeln Trojaner, wieder andere entwickeln Ransomware oder kümmern sich nur um Lösegeldabwicklung.

Compliance und die Business Continuity sind daher wichtige Aspekte für den Bestand eines Unternehmens. Die IT-Security gehört zu jeder Planung und Maßnahme in der IT und ist grundlegend für das Unternehmen. Aber es geht nicht nur um die IT, sondern um die gesamte Informationssicherheit. Jedoch gilt es die Balance zu wahren, zwischen Sicherheit und Arbeitsfähigkeit und Anpassungsgeschwindigkeit Letztlich geht es um das Ziel der *Resilienz* im Unternehmen.

Was heißt das für das Management?

Wenn also die Informationssicherheit ein Infinite Game ist, heißt das für die Informationssicherheit im Kontext des Unternehmens, dass man auf einem Infinite-Spielfeld kein Finite-Spiel (oder Business) spielen kann, ohne seine Resilienz zu verlieren. Sei es im Hinblick auf die IT-Sicherheit, Informationssicherheit oder auch im Business. Das Spiel geht immer weiter und man muss flexibel bleiben, um dem zu folgen. Bitter ist, dass man aus dem Spiel auch nicht aussteigen kann.

Zudem muss man akzeptieren, dass man nicht allen Bedrohungen vorauseilend begegnen kann, etwa solchen, die man noch nicht kennt. Und man hat auch nicht für alle Themen laufend die richtigen Mitarbeiter, Technologien, Organisationen und Budgets an der Hand. Es gilt, sein internes Mindset neu zu justieren, das die Informationssicherheit nicht nur als Risiko sieht, sondern die Herausforderung als fördernd im Sinne der Unternehmensentwicklung zu akzeptieren.

Welche Bausteine für laufende Anpassungsfähigkeit?

Wenn es im ständigen Wandel des Infinite Game also nicht den einen Schalter gibt, um in der stetig wechselnden Umwelt bestehen zu können, wie bekommt man das Problem in den Griff? Wir empfehlen, alle folgenden Bausteine anzuwenden:

1. Vision formulieren, für die man steht

Arbeiten Sie mit ihren Mitarbeitern an einer Vision im Bereich der Informationssicherheit, die nicht Selbstzweck ist, sondern deren Inhalte und Ziele für jeden Mitarbeiter klar, verständlich und nachvollziehbar sind. Und mit denen er sich identifizieren kann, nicht um der Vorgesetzten oder der Regeln willen, oder aus Angst vor Strafen, sondern um des gemeinsamen Zieles willen. Auch wenn das Ziel „absolute Sicherheit“ letztlich nie erreicht wird, kann die graduelle Annäherung und stetige Fortentwicklung sich als Motivation für die Mitarbeiter zeigen. Und die Visionen müssen top down vorgelebt und erfahrbar sein, sie müssen zur Kultur der Organisation passen. Nur dann werden sie gelebt und erfüllt.

2. Couragierte Führung

Das Management muss bei der Informationssicherheit mit gutem Beispiel voran gehen und motivieren, es muss sowohl kurzfristige als auch langfristige Ziele verfolgen, die dem Unternehmen dienen und auch den einzelnen Mitarbeitern. Das ist nicht immer einfach, denn Regeln und Maßnahmen einzuführen, Investitionen oder Technologieentscheidungen auszubalancieren, ist eine stetige Herausforderung, auch unter dem Blickwinkel der Interessen der verschiedenen Stakeholder. Als operationalisiertes Ziel der Führung kann die Einführung eines Informationssicherheitsmanagementsystems (ISMS) auf Basis von ISO 27001 oder Tisax dienen. Dies ist eine sehr pragmatische Aufgabe, schafft die Erteilung eines Zertifikats doch ein klares Ergebnis, das intern und extern mehr Sicherheit bringt, von Kunden gefordert wird oder vom Markt als positives Signal wahrgenommen wird.

3. Kultur des Vertrauens und des Wissens

Was ist gemeint? Das möchten wir anhand einer kurzen Handlungsanweisung erläutern: „Intelligente Anwendung der kommunizierten Vereinbarungen“. Das nötige Wissen und die Awareness sind ein wichtiges Ziel. Dem Mitarbeiter werden die nötigen Kenntnisse vermittelt und das Engagement zugetraut, dass er genau überlegt, was er tut und prüft, was im Sinne des Unternehmens ist. Und wenn er unsicher ist, weiß er, wen er ohne Probleme befragen kann. Die Mitarbeiter müssen also Regelwerke und Vereinbarungen (Vorgaben, Standards wie ISO 27001, Tisax) haben, die ihnen erläutert werden müssen, damit sie danach handeln können. Die Regelwerke müssen daher angemessen sein, dem Stand der Technik entsprechen, sind stetig weiterzuentwickeln und zu kommunizieren. Der Mitarbeiter erhält die Wertschätzung, dass er persönlich als Teil des Unternehmens und Teams mitverantwortlich sein kann und seinen Beitrag leistet. Er schützt damit sein Unternehmen, seine Assets und den Arbeitsplatz vieler Kolleginnen und Kollegen, letztlich auch seinen eigenen.

4. Wettbewerb mit anderen

Letztlich müssen Organisationen im Markt bestehen und brauchen Kapital für den Betrieb, sie müssen Produkte und Dienstleistungen produzieren, verkaufen und laufend optimieren, ihre Mitarbeiter angemessen entlohnen, dabei auch wirtschaftlich handeln und die Kundeninteressen beachten. Informationssicherheit ist im Wettbewerb aber keine Last, die man ungestraft vernachlässigen kann, sondern ein Asset, dessen Erreichung ein Ansporn sein sollte.

5. Flexibilität im Handeln

In der Informationssicherheit als Infinite Game ändert sich laufend etwas, daher gilt es, sich so flexibel aufzustellen, dass man Bedrohungen bewältigen kann, auf Technologien reagieren um mit dem passenden Personal gezielt zu antworten. Ein gutes Beispiel dafür ist die Pandemie, denn mit Covid waren quasi von heute auf morgen 80 Prozent der Mitarbeiter im Home-Office: ein nie erprobtes und gekanntes Maß an Remote Working! Sie mussten also anders als bisher reagieren und Flexibilität und Geschwindigkeit waren Trumpf.

Es stellen sich Fragen wie „Make or Buy?“: So kann z. B. ein externer Informationssicherheitsbeauftragter bei mittelständischen Unternehmen viel bewirken, ohne dass zusätzliche Kapazitäten aufgebaut werden. Oder Sie nutzen ein externes Security Operations Center (SOC), das ihnen bei rechtzeitiger Vorbereitung schnell mit der passenden Expertise helfen kann, die intern ggf. nicht oder nicht schnell genug vor- ›››

liegt oder dann andere wichtige Aufgaben vernachlässigt. Seien Sie also flexibel in Ihren Handlungen, überdenken Sie Organisation und Konzepte und entwickeln Sie – je nach Kontext und Kritikalität – eine auf Ihr Haus angepasste Strategie.

6. Standards und Konzepte

Nutzen Sie gängige Ansätze, es bestehen vielfältige Technologien, Konzepte und Standards. Hier einige Beispiele:

- **Zero Trust Security Model:** Das Vertrauen in einen sicheren Zugriff ist fraglich in einer Zeit, in der auf Systeme und Daten von überall her und über diverse Medien erfolgt. Angesichts eines nunmehr als potenziell gefährdet angesehenen Netzwerks geht man erst einmal davon aus, besser niemandem zu trauen (*Zero Trust*) und schafft eine passende Architektur. Dieses Modell gilt als hochgradig sicher und kommt bei der Durchsetzung genauer und restriktive Zugriffsentscheidungen bei jeder Anfrage in Informationssystemen und -diensten zum Einsatz.
- **Security by Design:** Eine ernsthafte Verbesserung der Sicherheit muss immer Überlegungen zur Vermeidung von Risiken beinhalten, um durch gutes Design einer Lösung oder passende Maßnahmen die Verhinderung eines Schadens zu ermöglichen oder ihn von Beginn an auszuschließen. So sollten Sicherheitsanforderungen an Soft- und Hardware schon während der Entwicklungsphase oder Einführung eines Produktes berücksichtigt werden, um spätere Sicherheitslücken zu verhindern.
- **Least Privilege Policy:** Eine Strategie, die auf die Reduzierung der Rechte aller Mitarbeiter auf ein Minimum setzt.
- **Defense in Depth:** Wie bei einer Zwiebelschale werden viele Schutzschichten um ein Asset definiert, um es bestmöglich zu schützen. Und wenn eine Schicht durchbrochen ist, bleiben noch weitere Schutzschichten.
- **Normen/Standards/ISMS:** Die Nutzung von Normen und Standards ist vorteilhaft, so fließen langjährige Erfahrungen und Kenntnissen von vielen Fachleuten ins Unternehmen ein. Und ein gut strukturiertes ISMS ist eine gute Grundlage zur wirksamen Umsetzung einer ganzheitlichen Sicherheitsstrategie. Es bietet Anleitungen für das Handeln in Notfällen. Hierbei bieten sich dem Management mehrere Optionen, die je nach Kontext der Organisation hilfreich sind, der international anerkannte Standard *ISO 27001* (bzw. für die Automobilbranche *Tisax*) oder der deutsche Standard des BSI *IT-Grundschutz*. Die Anwendung dieser Standards bietet nicht nur die Möglichkeit der Zertifizierung, sondern auch Hilfen für die Verbesserungen der Organisation.

7. Verhalten anpassen

Gehen Sie davon aus, dass in Infinite Games immer Dinge passieren, die bisher noch nicht oder noch nicht in dieser Dimension dagewesen sind, sowohl technisch als auch zeitlich oder auch organisatorisch. Wenn eine Situation für alle neu ist, braucht es Zeit, sich darauf einzustellen. Haben Sie keine Angst vor Unwissenheit. Bleiben Sie flexibel, ziehen Sie bei Bedarf externe Unterstützung heran, nutzen Sie Foren bzw. spezialisierte Security-Dienstleister.

Fazit: Die o.g. Aufgaben innerhalb der Bausteine sind nicht einfach zu lösen, unter dem Diktat von Zeit, Budget und personeller Kapazitäten gilt es Kompromisse einzugehen. Eine perfekte Lösung gibt es nicht. Und man sollte sich immer vor Augen halten, dass man sich mit hohem Engagement für die Informationssicherheit im Unternehmen nicht immer nur beliebt machen wird, da sich widersprechende Ziele (z.B. Sicherheit vs. Produktion) nicht ungewöhnlich sind.

Die Informationssicherheit ist kein Nebenkriegsschauplatz der Digitalisierung. Sie ist die Basis, ohne sie geht es nicht. Vertrauen ist schnell verspielt, wenn Vorfälle passieren, die nicht angepackt, gelöst und für die Zukunft vermieden werden. Vertrauen zurückzugewinnen, dauert länger als es zu erhalten, und manchmal ist es nicht wieder herstellbar. Lassen Sie es daher nicht so weit kommen! ■

INFORMATION & SERVICE

LITERATUR

S. Sinek: The Infinite Game: How Great Businesses achieve Long-Lasting. Portfolio Verlag, 2020

AUTOR

Klaus Kilvinger ist Geschäftsführender Gesellschafter und Berater der Opexa Advisory GmbH, einem auf Informationssicherheit spezialisierten Managementberatungsunternehmen mit Sitz in München.

KONTAKT

Klaus Kilvinger
klaus.kilvinger@opexa.de