IT-Infrastrukturen systematisch schützen und Risiken mindern

Dass die Sicherheit ein zentraler Aspekt der IT-Infrastruktur darstellt, hat inzwischen jeder verstanden. Meist fehlen jedoch das nötige Wissen und die Erfahrung, um eine holistische, strategisch ausgerichtete IT-Security zu gewährleisten. Hand bietet der IKT-Minimalstandard des BWL.

Das Bundesamt für wirtschaftliche Landesversorgung (BWL) hat einen Leitfaden zur Verbesserung der IKT-Resilienz entwickelt. Das Ziel ist die Minimierung des Risikos von Cyberattacken auf kritische Infrastrukturen. Dieser IKT-Minimalstandard basiert auf dem NIST CSF (Cyber Security Framework) und ist grundsätzlich für jedes Unternehmen oder jede Organisation nicht nur empfehlenswert, sondern notwendig. Die möglichen Konsequenzen einer Cyberattacke sind weitestgehend bekannt: Sensitive Geschäftsdaten werden verschlüsselt, Finanz- und Personendaten werden im Darknet zum Verkauf angeboten. Die Resultate jahrelanger Forschung sind plötzlich öffentlich einsehbar und stehen der Konkurrenz zur Verfügung. Ganz zu schweigen von Bussen, Schadensersatzklagen und existenzbedrohenden Reputationsschäden. Trotzdem wird das Thema Security in vielen Fällen immer noch zu stiefmütterlich behandelt, als dass es einen effektiven Nutzen hätte.

Wenn man OODA als Blaupause verwendet, ist es möglich, systematisch Risiken zu mindern, Prozesse zu verbessern und Sicherheitsvorfälle früh zu erkennen und zu bekämpfen.

Verwundbarkeitsanalyse

Die unternehmensspezifische Security-Strategie ist bei der heutigen Cyber-Bedrohungslage entscheidend. Das IKT-Minimalstandard-Assessment-Tool bietet ein Werkzeug, um ein Ergebnis zu erreichen, bei dem die Cyber-Sicherheitsrisiken und das Verbesserungspotenzial für Ihr Unternehmen identifiziert werden. Ziel ist der Aufbau und oder Erhalt eines auf individuelle Bedürfnisse zugeschnittenen Schutzniveaus.

Wie es um die Sicherheit der eigenen Informations- und Kommunikationsinfrastruktur steht, findet man am besten mit einer Verwundbarkeitsanalyse heraus. Eine Möglichkeit, die Ergebnisse aus dem IKT-Minimalstandard-Assessment richtig zu interpretieren, basiert auf dem OODA Loop. Dieses Konzept beschreibt einen Informationszyklus, der dabei helfen kann, Entscheidungsprozesse möglichst schnell zu durchlaufen. Der Militärstratege John Boyd hat die sogenannte OODA-Schleife als Framework für die schnelle Entscheidungsfindung während Kampfhandlungen entwickelt.

Der Autor
Franck Bouchoux, Senior Security Consultant, Netcloud

Der OODA Loop ist eine prägnante Darstellung des natürlichen Entscheidungszyklus. Er dient der Identifizierung, Visualisierung, Priorisierung und Orchestrierung der Abwehr bei den meisten Cyber-Bedrohungen. Dieser Loop wird heute auch in vielen anderen Bereichen angewendet und ist ein sehr gutes Beispiel für den kontinuierlichen Prozess, der für effektive Informationssicherheit erforderlich ist.

Der OODA Loop ist in vier Schritte gegliedert und lässt sich wie folgt auf die heutigen Praktiken des Cyber-Risikomanagements anwenden:

Schritt 1: Observe (Beobachten)

Cyberrisiken müssen minimiert werden. Um zu verstehen, welche Massnahmen dafür erforderlich sind, ist die Beobachtung der erste Schritt. Dies setzt äusserste Wachsamkeit voraus. Diese Phase liefert die Basis für die Definition der ICT-Strategie. Alle Informationen werden methodisch zusammengetragen und für die Analyse aufbereitet. Das Ziel ist das Sammeln von spezifischen Informationen. Dies bildet die Grundlage für die Beurteilung des IKT-Minimalstandards zur Verbesserung der ICT-Resilienz.

Schritt 2: Orient (Orientieren/Analysieren)

Nach der Beobachtung folgt das Analysieren. Die gewonnenen Informationen aus der GAP-Analyse nach dem IKT-Minimalstandard-Framework dienen dazu, die Situation richtig wahrzunehmen und sich anhand dieser Informationen zu orientieren.

Die Kombination des OODA-Loop-Modells mit Cyber-Risikomanagement-Tools ermöglicht es, interne Sicherheitsinformationen und Daten zu externen Bedrohungen in einen Kontext zu stellen. Nur so ergibt sich eine ganzheitliche Sicht der Risikohaltung über die Technologie, den Faktor Mensch und Prozesse hinweg. Auf diese Weise können Sicherheitsverantwortliche feststellen, welchen unmittelbaren Bedrohungen sie ausgesetzt sind.

Schritt 3: Decide (Entscheiden)
Auf Basis der Orientierung folgt nun das Entscheiden. Welchen Weg schlägt man ein, welche Strategie verfolgt man? Gestützt auf eine Risiko-Impact-Analyse werden Sofortmassnahmen definiert. Diese dienen dazu, die kritischsten Business-Prozesse von Unternehmen und Organisationen zu schützen. Und zwar mit grösstmöglicher Risikominderung bezüglich der aktuell gefährlichsten Bedrohungsakteure. Das Ziel ist, sich auf Risiken zu konzentrieren, die das Unternehmen bedrohen, um den Entscheidungsprozess erheblich zu beschleunigen.

Schritt 4: Act (Handeln)
Der letzte Part im OODA Loop ist das Handeln. Nach der gefällten Entscheidung folgt nun das praktische Handeln. Eine realistische Umsetzungsplanung unter Einbezug von Personen, Prozessen und Technologien ist unabdingbar. Die Implementierung der Massnahmen sollte nach Möglichkeit in Etappen geplant werden. Auch der Faktor Mensch muss beim Handeln berücksichtigt werden. Die Sensibilisierung der Mitarbeitenden ist ein steter Prozess, der neben den ganzen anderen getroffenen Massnahmen nicht zu vernachlässigen ist.

> Um nicht erpressbar zu sein, sind kluge Entscheidungen notwendig. Das Risiko so gering wie möglich zu halten sollte ein Muss sein.

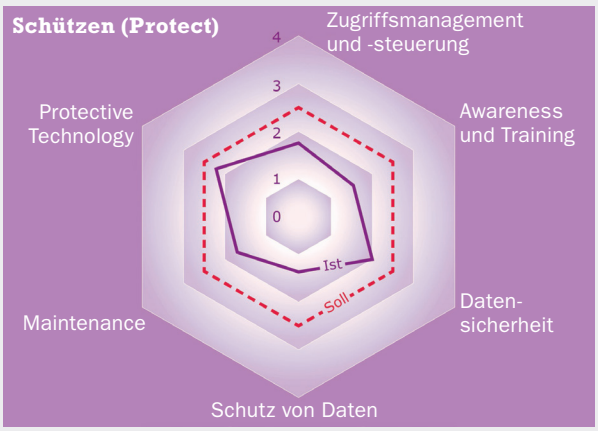
OODA als Blaupause
Der OODA Loop ist ein immer wiederkehrender Prozess, der auf Bereiche wie Business Continuity, Disaster Recovery, Cloud Security oder den Datenschutz generell anwendbar ist. Wenn man OODA als Blaupause verwendet, ist es möglich, systematisch Risiken zu mindern, Prozesse zu verbessern und Sicherheitsvorfälle früh zu erkennen und zu bekämpfen.

Bei der Durchführung eines sauberen IKT-Minimalstandard-Assessments sollte eine externe Instanz ins Spiel kommen. Ein erfahrener Security Consultant versteht den gesamten Prozess rund um das Assessment. Zudem ist er in der Lage, die Daten objektiv zu erheben und auszuwerten. Gestützt auf seine Expertise, hilft er bei der Interpretation und Beantwortung des Fragenkatalogs innerhalb des Assessments. Auch bei der Formulierung sowie der Umsetzung der Massnahmen kann ein Experte Hand bieten. Grundsätzlich müssen diese Massnahmen nicht teuer sein. Bei einem Sicherheitsvorfall kann beispielsweise eine Checkliste helfen, die richtigen Reaktionen auszulösen, um verschlüsselte Systeme zu isolieren. Man kann auch zu Testzwecken Angriffe simulieren. Das Ergebnis ist in jedem Fall eine klare Handlungsanweisung.

Um nicht erpressbar zu sein, sind kluge Entscheidungen notwendig. Das Risiko so gering wie möglich zu halten sollte ein Muss sein. Kein Unternehmen möchte sein Business und seine Kunden wegen eines Angriffs gefährden. Ein systematischer Schutz muss hier das oberste Gebot sein. Eine regelmässige Überprüfung, ob der IKT-Minimalstandard noch gegeben ist, muss in der Strategie fest verankert sein. Mit nur einem Assessment und den daraus abgeleiteten Handlungsanweisungen erreicht man keinen dauerhaften Schutz.

Sehen wir den Tatsachen ins Auge. Die Bedrohungslage ist allgegenwärtig. Eine Endpoint-Protection-Software und eine Firewall alleine schützen Ihr Unternehmen nicht angemessen. Handeln Sie jetzt!

IKT-MINIMALSTANDARD-ASSESSMENT-TOOL: AUSWERTUNG AM BEISPIEL «SCHÜTZEN»



Bei allen Themen geht es gleichermassen um Menschen, Technik und Prozesse. Das richtige Zusammenspiel bringt am Ende den richtigen Schutz.

- Zugriffsmanagement und -steuerung: IAM-Prozess, Fernzugriff, logische und physische Trennung der Infrastruktur, Multifaktor-Authentifizierung.
- Awareness und Training: Ist nicht mit einem simulierten Angriff zu verwechseln. Das Bewusstsein auf allen Ebenen ist entscheidend; Rolle, Verantwortung, Benehmen.
- Datensicherheit: Hier geht es um die eigentlichen Werte (C.I.A.) von Informationssicherheit; konkret Kapazität, Redundanz, Verschlüsselung, Datenlöschung, Trennung von Entwicklungsumgebung, Test und Produktion bzw. Anonymisieren von Daten.
- Schutz von Daten: Standard-Konfiguration, Asset Life Cycle, Change Management, Back-up und Restore Tests, Wiederherstellungspläne, Entsorgungskonzept, Technologieaustausch mit Partnern, Informationssicherheitsvorgaben im HR-Rekrutierungsprozess, Schwachstellenmanagement.
- Maintenance: Wartung und Reparaturen aufzeichnen, zeitnah und mit geprüften Mitteln unautorisierte Zugriffe vermeiden.
- Protective Technology: Logs-Aufzeichnung und -Überprüfung, Regelungen zum Einsatz von Wechseldatenträgern, Systemhärtung und DNS Security, Proxy, IDS, IPS, Segmentierung, Baseline und Abnahmetests.

Den Beitrag finden Sie auch online
www.netzwoche.ch