Büchner Barella
Sichert Unternehmen seit 1922

IN KOOPERATION MIT:
BOSCH
CyberCompare

CYBER-RISIKEN BEHERRSCHBAR MACHEN

ROADMAP DER CYBERSICHERHEIT

PREFERRED IHA PARTNER

Cybersicherheit ist in vieler Munde und betrifft jedes Unternehmen. Doch werden dabei immer alle relevanten Themen bedacht? Welche Budgets und welche Vorlaufzeiten werden überhaupt benötigt? Wir zeigen Ihnen die wichtigsten Eckpunkte auf, damit Sie Ihr Projekt von Beginn an strukturiert zum Erfolg führen können.

Der aktuelle Bosch CyberCompare Cybersecurity Benchmarkreport 2023 hat gezeigt, dass die meisten Unternehmen aktiv an konkreten Maßnahmen zur Erhöhung des Absicherungsniveaus arbeiten.

Nun unterscheiden sich typische Projekte im Bereich Cybersicherheit zunächst nicht unmittelbar von klassischen IT-Projekten. Es muss priorisiert werden, man benötigt die richtigen und ausreichenden Ressourcen in Form von Kapazitäten und Budget, eine gute Planung ist entscheidend und es sollte regelmäßig der Status Quo bewertet werden (z.B. mittels PDCA), um die jeweilige Aktivität auch zielgerichtet abzuschließen.

In der Praxis stellen wir fest, dass Security-Projekte allerdings oft noch on-top auf eine meist schon stark ausgelastete IT-Organisation treffen. Denn: Klassische IT-Infrastrukturprojekte, oder z.B. ERP Aktivitäten sind nicht neu – dafür ist die IT meist kapazitativ aufgestellt. Trotz der stark angestiegenen Cyber-Bedrohungslage ist jedoch in den meisten Unternehmen nicht in zusätzliche Expertise und Betriebskapazität in den IT-Teams investiert worden: Auf ca. 1.000 MitarbeiterInnen entfällt im Schnitt nur ca. eine Vollzeitstelle mit Security-Expertise.

Schauen wir also auf drei relevante Faktoren, welche für Sie bei der Ausplanung Ihres Cybersicherheitsprogramms hilfreich sein können:

1. Prioritäten für den Mittelstand – wesentliche Handlungsfelder
2. Welche Budgets sollten eingeplant werden?
3. Welche Vorlaufzeiten müssen berücksichtigt werden?

1. Prioritäten für den Mittelstand – wesentliche Handlungsfelder

Wie immer gilt: jedes Unternehmen ist anders. Das individuelle Geschäftsmodell, der oft zitierte Risikoappetit und natürlich die Ist-Ausgangssituation in der IT- und OT-Security sind so unterschiedlich, dass es pauschal immer falsch ist, ungeprüft „Top 10 Listen" abzuarbeiten.

Daher sollte der Start eines Cybersicherheitsprogramms immer mit einer Risikoanalyse (Was sind die wesentlichen Bedrohungen für mein Unternehmen oder meine Geschäftseinheit?) und einer Bestandsaufnahme erfolgen. Ideal, wenn dies in Anlehnung an relevante Standards wie die ISO27001 (z.B. auf Basis der BSI-Grundschutz-Richtlinien) durchgeführt wird, da so alle relevanten Themenfelder berücksichtigt werden.

TIPP Prüfen Sie die Ergebnisse Ihrer Bestandsaufnahme hinsichtlich der acht folgenden Security-Themen und bewerten Sie mögliche Lücken. Alle acht Themenkomplexe bewerten wir als „Pflicht" und sollten – wenn nicht bereits geschehen – in Ihren Fokus rücken.

1

Schwachstellenmanagement

Ein PenTest, welcher nicht nur extern Ihre IP-Adressen scannt und die externen Perimeter testet, sondern auch intern die IT-Infrastruktur angreift, ist aus unserer Bewertung heraus ‚Pflicht'. Tatsächlich führt dies auch oft zu mehr Verständnis in der Geschäftsführungsetage für notwendige Investitionen in Personal und Technik, um das Security-Niveau auf einen angemessenen Stand zu heben. Die Komplexität einer IT eines mittelständischen Unternehmens wird immer kritische Schwachstellen produzieren: Seien es fehlerhafte Konfigurationen, zu weitreichende Berechtigungen oder nicht gepatchte Schwachstellen. Dazu lohnt sich auch der Einsatz eines Schwachstellenscanners, mit dem z. B. monatlich ein Abgleich mit den aktuell hoch priorisierten Schwachstellen und verfügbaren Patches durchgeführt wird. Hier gibt es zum Einstieg auch Open Source Tools. bleiben.

2

Mitarbeitersensibilisierung

Belassen Sie es nicht bei einem einmaligen Phishing Test. Das kommt in der Regel beim Team nicht so gut an. Lieber regelmäßig (z.B. einmal pro Quartal) und v.a. dann mit einem guten, kurzen Security-Training kombinieren. Das ist sicherlich viel effektiver als eine jährliche umfangreiche Pflichtschulung

3

Endpoint Security Lösungen

Sie nutzen noch eine klassische Antivirus-lösung, um Ihre Endgeräte zu schützen? Die Funktion ist zwar weiterhin relevant und lebt auch weiter, allerdings in modernen Endpoint Security Lösungen. Diese bringen nicht nur verbesserte Detektionsfähigkeiten mit, sondern auch eine Response-Funktion, um im Verdachtsfall auch schnell, adäquat und automatisiert zu reagieren. Daher nennen sich diese Produkte Endpoint Detection & Response (EDR) und es gibt sie auch in der Variante wie X-tended Detection & Response (XDR), bei der auch weitere Systeme in die Analyse inkludiert werden. Hier sollten Sie sich dringend mit einem Upgrade beschäftigen.

4

Netzwerksicherheit

Kein neues Thema, aber oftmals noch nicht bestmöglich aufgestellt. Dazu zählen wir moderne Firewallsysteme (externer Perimeterschutz und interne Firewalls z.B. an der Trennung zwischen IT und OT), und v.a. auch das äußerst effektive Werkzeug der Netzwerksegmentierung. Jedes Segment reduziert bei einem leider jederzeit möglichen Cyberangriff die Auswirkungen, da der Angreifer jeweils mehr Zeit investieren muss, um in weitere Segmente vorzudringen. Denken Sie dabei über das klassische eigene Segment für die Drucker und das Gäste-WLAN hinaus und nehmen Sie sich v.a. auch in der Produktion externe Expertise dazu, um die spezifische Herausforderung der Altsysteme in der OT bestmöglich zu kapseln. Zu einer State-of-the-art Architektur gehören dann noch die Themen der verschlüsselten Kommunikation und Kommunikation zwischen den Schichten bis in die Cloud.

5

Cloud

Bleiben wir beim Sichtwort Cloud: Nach wie vor ist es sicherlich auch eine Philosophiefrage, ob man seiner onPremise IT mehr vertraut als den Milliarden USD, welche die großen Cloud-Hyperscaler jährlich in Securitymaßnahmen investieren. Da auf der Anwendungsebene durch den Software as a Service Boom der letzten 10 Jahre und die Microsoft 365 Strategie ein zumindest partieller Cloud-Einsatz mittlerweile faktisch notwendig ist, muss sich jedes Unternehmen auch mit Cloud-Security auseinandersetzen: Starten Sie damit, die Konfiguration der Cloudzugriffe durch externe Expertise bewerten und ggf. justieren zu lassen. Und: Mehrfachauthentifizierung (MFA), wo es nur möglich ist! Falls noch nicht umgesetzt, sollten privilegierte Konten (Admins), Fernzugriffe und Zugriff auf sensible Daten priorisiert mit einem zweiten Faktor geschützt werden.

6

Recovery & Business Continuity

Wie bereits in Bezug auf die Netzsegmentierung geschrieben: Wir wissen, dass Angriffe leider nicht vollständig ausgeschlossen werden können. Daher sollten auch eine Aufrüstung Ihrer Recovery & Business Continuity im Fokus stehen. Starten Sie z.B. mit dem strukturierten Aufsetzen eines Bereitschaftsdiensts, damit Sie in Krisensituationen nicht zu stark auf das Prinzip ‚Hoffnung' setzen müssen. Dieser Bereitschaftsdienst ist dann Teil des Notfallplans. Der sollte möglichst aktuell gehalten und pragmatisch umgesetzt sein. Sie müssen in der Krise den Plan schnell effektiv einsetzen können. Dokumentieren Sie dort auch zumindest kurz, welche geschäftskritischen Prozesse in welchen Fachbereichen betroffen sein könnten. Als ideal hat sich herausgestellt, wenn Unternehmen den Plan alle 1-2 Jahre einmal üben: Szenario Ransomwareangriff und dann einen halben Tag im Workshop die Aktivitäten durchspielen. Dies ist ein sehr effektives Mittel, die Awareness im Krisenstab zu erhöhen und den Notfallplan auf Lücken zu testen. Abschließend der entscheidende Faktor, ob Cyberangriffe „gut" überlebt werden können: Die Qualität des Backupkonzepts. Tipp: gerne auch mit einem PenTest auf mögliche Schwachstellen hin testen. Und: den Notfallplan auch ausdrucken.

7

Rechte/Rollen und Authentifizierung

Die Wichtigkeit eines guten Berechtigungskonzeptes im Kontext von möglichen Cyberangriffen muss nicht separat betont werden. Identity und Access Management (IAM), Privileged Access Management (PAM), Multi-Faktor-Authentifizierung (MFA) und integrierte Single-Sign-On-Lösungen (SSO) sollten nicht nur wohlklingende Abkürzungen bleiben, sondern verdienen ein ganzheitliches Konzept, bei welchem idealerweise auch wieder die Risikoanalyse zur Hand genommen und dann risikobasiert kritische Systeme entsprechend zusätzlich abgesichert werden.

8

Managed Services

Welches Feld wächst bei den meisten Security-Anbietern sehr stark? Die Managed Services, also die vertraglich geregelte operative Übernahme von Services. Beispielsweise für eine Endpoint Security Lösung (Unsere Empfehlung!), für die Firewall, oder gleich für ein ganzes Security Operations Center (SOC).

Schnell landen Kosten im 6-stelligen EUR-Bereich pro Jahr – dennoch lohnt es sich als mittelständisches Unternehmen meist, unter Berücksichtigung der Gesamtkosten, spezifische Expertise zuzukaufen, anstatt sie jeweils immer selbst intern abzubilden. Ein SOC im Eigenbetrieb ist in der Regel nur für Großunternehmen stemmbar.

2. Welche Budgets sollten eingeplant werden?

Cybersicherheit kostet Geld, erst recht, wenn Sie weiter aufgerüstet werden soll. Und ähnlich wie bei Feuerschutztüren oder einer zweiten redundanten Internetanbindung: Die Vorteile werden Sie leider nicht unmittelbar positiv im Betriebsergebnis des Unternehmens sehen.

Sprich, ein ‚Return on Invest' ist immer schwer herzuleiten. Am einfachsten kann dies wahrscheinlich über die Reduzierung von Versicherungsprämien oder das Aufzeigen von tatsächlichen Schadensummen bei erfolgreichen Angriffen auf ähnliche Unternehmen erfolgen. Bei Bedarf unterstützen wir Sie hier sehr gerne.

Wenn Sie für einen bestimmten Service auf einen passenden Anbieter zugehen und die Frage nach einer initialen Budgetschätzung stellen, werden Sie vermutlich erstmal Scoping-Workshoptermine als Antwort erhalten. Denn klar: Der Preis steht und fällt mit den Anforderungen und dem definierten Scope.

Dennoch sehen wir in unseren vielen Ausschreibungsprojekten wiederkehrende Auftragswerte und Durchschnittswerte bei vergleichbaren Anforderungen. Die nachfolgende Tabelle greift wichtige Services und Lösungen aus Kapitel 1 („Top 8") auf und beschreibt die Kostenspanne, die wir typischerweise in den Projekten sehen und die wir unserer CyberCompare Preisdatenbank entnommen haben.
Als Annahme haben wir die Zahlen auf ein mittelständisches Unternehmen mit 2.000 Mitarbeitenden und 2.000 Clients bezogen.

ANGEBOT Wir erarbeiten für Sie gerne eine individuelle Kostenschätzung Ihres Cybersicherheitsprogramms auf Basis weniger Eckdaten.

Service	Kostenspanne
Strategie: Risikoanalyse, Diagnostik, Audit (inkl. OT)	• Diagnostik: 2.000 – 7.000 EUR • Audit: 9.000 – 20.000 EUR
Schwachstellen: PenTest + Schwachstellenscans	• Initialer PenTest: min. 10 Tage, Max. 25 Tage: 13.000 – 33.000 EUR Schwachstellenscanner, ggf. gekoppelt mit Managed Service: 10.000 – 120.000 EUR / Jahr
Sensibilisierung: Awareness & Trainings	• Awareness Plattform: Ca. 1,40 EUR / User / Monat • Für 2.000 User ca. 33 TEUR p.a.
Endpoint Security: EDR / EPP / XDR	• EDR / XDR ca. 1,50 – 4 EUR / Monat / Endpunkt Mittelwert 2,50 EUR • Für ca. 2.000 Endpunkte ca. 36.000 – 100.000 EUR p.a. Mittelwert ca. 60.000 EUR p.a.
Monitoring übergreifend: SIEM / SOC	• Mittelwert ca. 170.000 EUR + ca. 50.000 EUR one-time
Outsourcing: Managed Service EDR (MDR)	• MDR inkl. EDR ca. 2,1 – 6,5 EUR / Monat / Endpunkt Mittelwert 4 EUR. • Für ca. 2.000 Endpunkte ca. 50.000 – 150.000 EUR p.a. Mittelwert ca. 100.000 EUR

3. Welche Vorlaufzeiten müssen berücksichtigt werden?

Der Disclaimer muss hier ähnlich lauten wie in Kapitel 2 zu den Kosten. Natürlich entscheidet auch bei der Einführungsdauer und der Vorlaufzeit v.a. der Umfang der angestrebten Lösung.

Aber auch hier gibt es wieder Erfahrungswerte, die sich in den verschiedenen Projekten oft bestätigen.

Als grundsätzliche Empfehlung geben wir wie initial beschrieben mit, den ersten Aufsatzpunkt immer in einer Diagnostik und Risikoanalyse zu definieren. Auf der Basis lässt sich dann eine Roadmap der angestrebten Maßnahmen aufstellen, welche mit Hilfe der Kostenschätzung aus Kapitel 2 auf Machbarkeit geprüft werden kann („Haben wir so viel Budget?").

Ist die Freigabe des Budgets erfolgt, sollte man zügig kritische Einzelthemen angehen, denn meistens sind nicht die externen Verfügbarkeiten die Limitierung im schnellen Vorgehen, sondern v.a. die intern fehlende Zu- und Mitarbeit.

Hinzu kommen auf der Anbieterseite notwendige Bearbeitungszeiten für Angebotserstellung, Beantwortung der Anforderungen, Klärung von Fragen und Terminfindung für notwendige Workshops. Eine etwas defensivere interne Planung ist also empfehlenswert.

TIPP Falls Sie von Anbietern, Systemintegratoren oder Resellern dazu gedrängt werden, möglichst schnell Verträge abzuschließen (evtl. mit Hinweis auf das ablaufende Geschäftsjahr und dadurch besonders attraktiven Konditionen), lassen Sie eher Vorsicht walten. Ein strukturierter Vergleich macht sich in jedem Fall für Sie als Kunde bezahlt und reduziert das Risiko.

Nachfolgend haben wir typische Zeitspannen für die zuletzt besprochenen Services und Lösungen aufgeführt:

Service / Produkt	Spezifikation (geschätzt)	Vorlauf (geschätzt)	Druchführung (geschätzt)
Risikoanalyse, Diagnostik	2-3 Wochen	Kurzfristig 2-6 Wochen	2 Wochen
PenTest	3-4 Wochen	2 Monate	4 Wochen
Awareness Programm	2-3 Wochen	Kurzfristig 2. Wochen	2 Wochen
Endpoint Security: EDR / EPP / XDR	4-7 Wochen	1-2 Monate	2-3 Monate
MDR / Managed SOC	6-9 Wochen	2 Monate	6 Monate Onboarding bis stabiler Betrieb

4. Fazit

Cybersecurity bleibt trotz – oder wegen – aller technischer Innovationen eine große Herausforderung.

Die Anzahl potentieller Lösungen und Service-Angebote übersteigt um ein Vielfaches die Möglichkeiten eines Unternehmens, da interne Kapazitäten und Budgets immer limitiert bleiben werden.

Aus unserer Sicht muss jedes Cybersicherheitsprogramm mit einer umfassenden Bestandsaufnahme und einer Risikoanalyse starten, welche idealerweise auch nicht allein aus der IT heraus gestartet wird.

Die identifizierten Lücken kann man danach strukturiert und schrittweise mit „Leben" füllen und konkrete Cyberlösungen anstreben. Die vorliegende Unterlage fasste dazu die aus unserer Erfahrung Top-Themen zusammen, welche mindestens mittelfristig Beachtung verdienen sollten. CyberCompare unterstützt Sie gerne auf dieser Reise von der Bestandsaufnahme, der gemeinsamen Roadmap-Entwicklung, Budgetindikationen bis zur Durchführung konkreter Security-Projekte mittels Markttransparenz und Angebotsvergleichen.

Dabei sind und bleiben wir immer unabhängig und zu 100% auf Ihrer Seite.

Vor über 100 Jahren gegründet, hat sich die BüchnerBarella Unternehmensgruppe zu einem der erfolgreichsten Gewerbe- und Industrieversicherungsmakler in Deutschland entwickelt.

Wir kennen uns in der Fabrik genauso aus wie im Büro; sind auf der Baustelle ebenso präsent wie in der Gesundheitswirtschaft. Mehr als 400 Expertinnen und Experten an 19 Standorten in Deutschland und der Schweiz arbeiten mit Leidenschaft, Hochdruck und Know-how an ganzheitlichen Risikoberatungsansätzen und intelligenten Versicherungsmanagement-Konzepten, damit Sie sich auch noch morgen auf Ihre Stärken konzentrieren können.

Das WIR ist das Besondere. Bei uns steht der Mensch im Mittelpunkt unseres Handelns. Das gilt für unsere Kunden und Partner genauso wie für unsere Mitarbeiterinnen und Mitarbeiter.

BüchnerBarella. 100 Jahre WIR für Sie.

PREFERRED IHA PARTNER

Ihr direkter Ansprechpartner:

GRAF ALEXANDER BERNADOTTE AF WISBORG

Leitung Verbände

+49 7221 9554-15

a.bernadotte@buechnerbarella.de