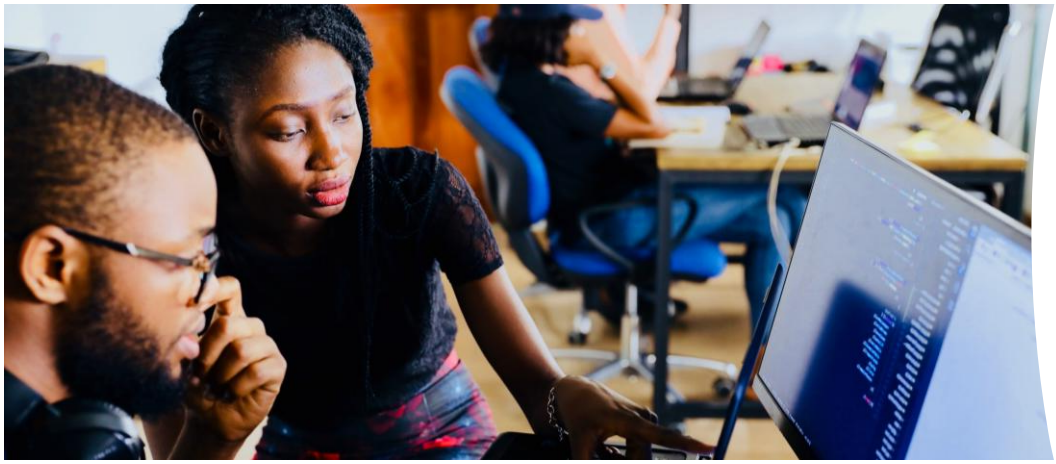


Asset Security Strategy Assessment

Laut Bitkom entsteht der deutschen Wirtschaft durch Cyber-Kriminalität ein jährlicher Gesamtschaden in Höhe von 289 Mrd. Euro. Nur 10 % aller Unternehmen in Deutschland blieben in den Jahren 2023 und 2024 von Cyber-Attacken verschont. 88 % berichten hingegen, dass Angriffe auf ihre Unternehmensnetzwerke stattgefunden haben.

Cyber-Kriminalität war schon immer ein Problem, dem sich spätestens mit dem zunehmenden Trend zu Remote Work und Home Office neue Angriffsflächen und Möglichkeiten erschlossen haben.

Gartner empfiehlt Führungskräften im Bereich Sicherheits- und Risikomanagement (SRM) in einer im April 2023 veröffentlichten Studie, bei der Entwicklung und Umsetzung von Cybersicherheitsprogrammen – im Einklang mit sieben wichtigen Branchentrends – die Balance zwischen Investitionen in Technologie und menschenzentrierten Elementen zu überdenken und sich dabei auf drei Schlüsselbereiche zu konzentrieren: (1) die wesentliche Rolle der Mitarbeiter für den Erfolg und die Nachhaltigkeit des Sicherheitsprogramms, (2) technische Sicherheitsfähigkeiten, die eine größere Transparenz und Reaktionsfähigkeit im gesamten digitalen Ökosystem des Unternehmens bieten und (3) die Umstrukturierung der Arbeitsweise der Sicherheitsfunktion, um eine höhere Agilität zu ermöglichen, ohne die Sicherheit zu beeinträchtigen.

Die sieben Trends von Gartner für SRM-Führungskräfte

Trend 1: Menschenzentriertes Sicherheitsdesign

Trend 2: Verbesserung des Personalmanagements für die Nachhaltigkeit von Sicherheitsprogrammen

Trend 3: Umgestaltung des Cybersecurity-Betriebsmodells zur Unterstützung der Wertschöpfung

Trend 4: Management des Bedrohungspotenzials

Trend 5: Immunität der Identitätsinfrastruktur

Trend 6: Cybersecurity-Validierung

Trend 7: Konsolidierung von Cybersicherheitsplattformen

Die Trends 1 und 2 betrachten hauptsächlich den Menschen und dessen Verhalten, die Trends 3 und 4 tragen den Anforderungen, die aus der zunehmenden Digitalisierung und den neuen Arbeitsmethoden resultieren, Rechnung und die Trends 5 bis 7 beschäftigen sich mit Techniken, Prozessen und Tools, wobei ein starker Fokus auf digitalen Identitäten, Governance und Access Management liegt.

Auch neue gesetzliche Vorgaben stellen Unternehmen vor gestiegene Erwartungen an die Cyber-Security. Die europäische NIS-2-Richtlinie beinhaltet bereits wesentliche Regelungen, die sich auch im deutschen IT-Sicherheitsgesetz 3.0 wiederfinden werden. NIS 2 erweitert die Befugnisse und Handlungsmöglichkeiten der national zuständigen Behörden. So kann das Bundesamt für Sicherheit in der Informationstechnik (BSI) künftig sogar Menschen, die als Geschäftsführung oder gesetzliche Vertreter für Leitungsaufgaben zuständig sind, die Wahrnehmung der Leitungsaufgaben vorübergehend untersagen, wenn diese den Anordnungen des BSI nicht nachkommen.

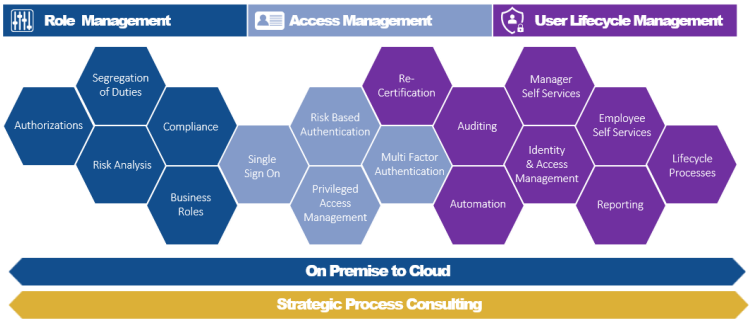
Governance und Compliance gehören zu den Hauptsäulen der NIS-2-Richtlinie und adressieren das Role Management, das Access Management und das User Lifecycle Management. In der Hauptsache geht es um Fragen der Autorisierung und Authentifizierung sowie um passende Berechtigungen. Dabei spielt das Access Management eine entscheidende Rolle. Ohne Multi-Faktor-Authentifizierung (MFA) sind Unternehmen deutlich anfälliger gegenüber Phishing-Attacken. Identity Management mit Single Sign-On und MFA sind kein Luxus, sondern eine unabdingbare Voraussetzung für das Management und die Steuerung von Identitäten, Zugriffen und Berechtigungen.

IBsolution GmbH | Im Zukunftspark 8 | 74076 Heilbronn | Deutschland
Telefon: 07131 2711 3000 | info@ibsolution.com | www.ibsolution.com

Handlungsfelder erkennen, Schwachstellen reduzieren

Es bleibt festzuhalten, dass die Themenfelder der Cyber-Security immer umfangreicher werden. Der Mensch bleibt die größte Schwachstelle und ist mit viel Training zu sensibilisieren. Je weiter man in den Layern voranschreitet, desto technischer und anspruchsvoller im Wirkungsgrad wird es. Wenn erst einmal privilegierte User übernommen sind, steht ein verheerender Angriff bevor. Jeder Layer hat seine Berechtigung in einem gesamtheitlichen Security-Konzept. Die letzte Instanz ist der Data Layer, den es laut Gartner mit allen Mitteln zu schützen gilt.

Role Management, Access Management und User Lifecycle Management erhöhen das Schutzniveau im Data Layer maßgeblich.



Im Rahmen unseres **Asset Security Strategy Assessments** erarbeiten wir in einem vielfach erprobten Vorgehen gemeinsam mit Ihnen eine Roadmap, die vorgibt, wie sicherheitsrelevante Themenfelder in Ihrem Unternehmen zukunftsorientiert und unter Beachtung Ihrer aktuellen Gegebenheiten bearbeitet werden müssen. Dabei betrachten und fokussieren wir einzelne Teilgebiete, die Sie vollumfänglich oder in Einzelbausteinen mit uns beleuchten und angehen können.

Asset Security Strategy Assessment @IBsolution

Basismodul
Asset Security Assessment — **6.000 €**

Das Basismodul Asset Security Assessment ist obligatorisch für unsere gesamte Workshop-Serie und liefert Ergebnisse, die für alle nachfolgenden Module relevant sind. Im Basismodul erhalten Sie eine Übersicht zu allen Unterthemen der Reihe. Dabei liegt der Fokus eher auf einer allgemeinen Betrachtung der genannten Module sowie auf der Erklärung ihrer Relevanz und gegenseitigen Beeinflussung.

Modul User Lifecycle Management: *Besprechung der Benutzerprozesse auf Basis standardisierter Best-Practice-Prozesse – mit Fokus auf On-Premise-SAP-Systemen und Microsoft Active Directory.*	**6.000 EUR**
Sub-Modul Anbindung zusätzlicher Systemtypen: *Integration zusätzlicher Systeme in die User Lifecycle Prozesse und Definition vollautomatischer Anbindungen.*	**2.000 EUR**
Sub-Modul Cloud und Microsoft Azure Provisioning: *Erweiterung der Betrachtung der On-Premise-Systeme um essenzielle Cloudsysteme aus der SAP-Welt oder um den Einsatz von Microsoft Azure bzw. Entra ID.*	**2.000 EUR**
Modul Role Management und SAP-Berechtigungen: *Bewertung Ihres SAP-Berechtigungskonzepts hinsichtlich Aktualität und SAP S/4HANA Readiness, Identifizierung von Lücken und Aufzeigen von Lösungswegen.*	**10.000 EUR**
Modul Businessrollen-Konzept: *Aufzeigen von Möglichkeiten, wie bei Ihnen ein Businessrollen-Konzept umgesetzt werden kann und wie Sie dadurch massiv Aufwände in der Berechtigungspflege reduzieren.*	**5.000 EUR**
Modul Access Management: *Mit Blick auf ihre aktuelle und zukünftige Systemlandschaft zeigen wir Möglichkeiten, wie Sie Single Sign-On (SSO), Multi-Faktor-Authentifizierung (MFA) oder auch risikoabhängige Zugriffe (RBA) im Unternehmen realisieren können.*	**2.000 EUR**
Modul Cyber Security Check: *Mit unserem 360 Degree Security Check for SAP Landscapes ermitteln wir im Rahmen eines zweitägigen Workshops den aktuellen Stand Ihrer IT-Sicherheit über alle relevanten Security-Layer hinweg und lokalisieren Schwachstellen.*	**10.000 EUR**
Modul Tool-Auswahl: *Auf Basis der definierten Prozesse und der fachlichen Anforderungen sowie unter Berücksichtigung der aktuellen Entwicklungen im IAM-Markt führen wir eine Tool-Auswahl mit besonderem Fokus auf die gängigen State-of-the-art-Lösungen für Sie durch und begründen die Ergebnisse nachvollziehbar.*	**4.000 EUR**

Gesamt: ~~47.000 EUR~~ 44.000 EUR

IBsolution GmbH | Im Zukunftspark 8 | 74076 Heilbronn | Deutschland
Telefon: 07131 2711 3000 | info@ibsolution.com | www.ibsolution.com