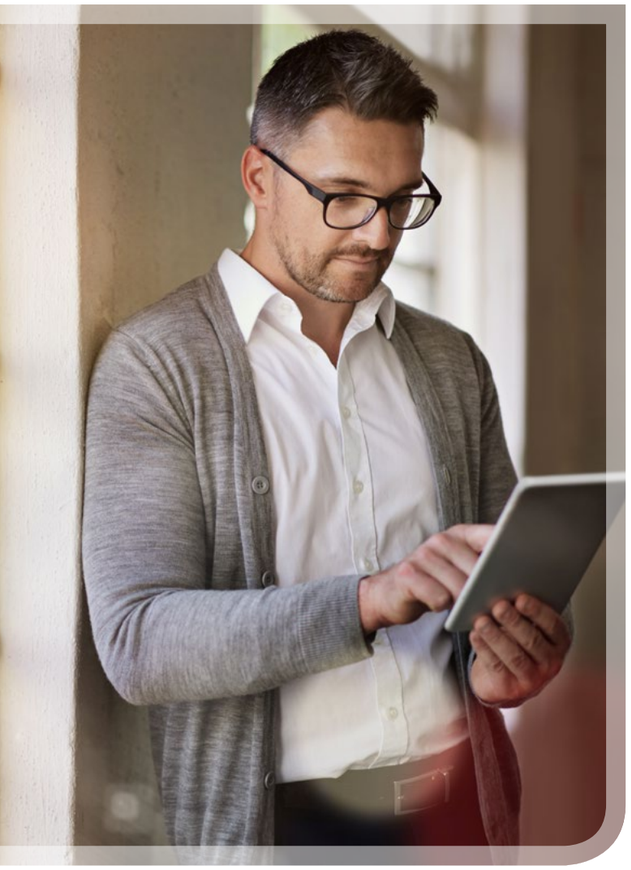
ALLES IST MÖGLICH – ABER SICHER

Secure Information



IT-SECURITY: ANWENDERFREUND UND BUSINESS-UNTERSTÜTZER

IT steckt überall drin. Von der kleinsten Mail bis hin zum größten ERP-System oder Rechenzentrum. Aber steckt auch immer die IT-Sicherheit mit drin? Eins ist klar: Nie zuvor waren Daten und Mitarbeiter so mobil und losgelöst von Standort und Gerät. Und nie zuvor waren die Grenzen zwischen Unternehmensnetzwerk und dem Rest der Welt so durchlässig.

Die Basis für jede Strategie: wissen, worauf es ankommt. Trends kommen und gehen. Einige aber bleiben. Zum Beispiel Social Media, Cloud Computing und Mobility. Hinzu kommen wachsende Entwicklungsfelder wie das Internet der Dinge, Industrie 4.0 und Machine-to-Machine-Communication. An diesen Trends kommen Unternehmen nicht vorbei. Und darauf muss sich auch die IT-Abteilung einstellen. Denn erst durch die richtigen Sicherheitskonzepte können Unternehmen die neuen Trends für ihr Business nutzen. Damit wird IT-Security zum zentralen Möglichmacher zeitgemäßer Geschäftsprozesse.

Eine weitere Herausforderung für moderne IT ist die verschärfte Bedrohungslage: Hackerangriffe, Wirtschaftsspionage, Datenlecks gehören zum Alltag – und nehmen ständig zu. So wird verlässlicher Schutz immer geschäftskritischer, auch angesichts des wachsenden Compliance-Drucks. Hinzu kommt: Sicherheitsvorfälle sind schlecht fürs Image. Deshalb muss Security von Anfang an integraler Bestandteil jeder IT-Lösung sein – ob im Rechenzentrum, am Arbeitsplatz oder im Netzwerk. Genau an diesen Stellen setzt unsere Stärke als IT-Dienstleister an: Wir kombinieren 15 Jahre Security-Erfahrung mit unserem Know-how über alle Bereiche der IT hinweg. Denn nur wer sich mit IT-Lösungen aller Disziplinen auskennt, kann diese auch sicher machen.

WORKPLACE SECURITY – PRAXISTAUGLICH UND UNSICHTBAR FÜR DEN ANWENDER

Ein Arbeitsplatz ist ein Arbeitsplatz ist ein Arbeitsplatz. Weit gefehlt! Heute arbeiten Mitarbeiter am Desktop, mit Notebook, Smartphone oder Tablet gleichermaßen. Sie wollen sich von überall und mit jedem Gerät mit dem Unternehmensserver verbinden, E-Mails schreiben, wichtige Daten abrufen, bearbeiten und mit anderen teilen. Und das können sie auch!

Die Arbeitswelt hat sich verändert: nicht zuletzt durch die Verlagerung von Daten in die Cloud, den Einsatz mobiler Endgeräte, Social Media und Webapplikationen. Anwender greifen heute nicht mehr nur von einem Gerät aus auf Unternehmensdaten zu. Manchmal nutzen sie auch ihre eigenen Geräte, auf denen dann private und berufliche Daten gleichermaßen gespeichert sind. Weil sie dabei nicht mehr zwingend im Büro sitzen, müssen auch immer mehr Zugänge zu den Daten geschützt werden. Kurzum: Es sind völlig neue Konzepte für die Workplace Security gefragt.

UNBEMERKT SICHER

Wichtig dabei ist die Benutzerfreundlichkeit für den Anwender. Denn ein Virenscan, der das Arbeiten vorübergehend unmöglich macht, ist für die User nicht akzeptabel. Zu einer guten Workplace Security gehört deshalb das Absichern aller Geräte, Zugänge und Daten, mit denen der Mitarbeiter arbeitet – ohne dass dieser etwas davon merkt.

WORKPLACE SECURITY – WAS GEHÖRT DAZU?

>>> PROTECTION
Wie man Geräte robuster gegen Schadsoftware und Angriffe macht, wissen wir genau. Gemeinsam finden wir passende Lösungen für:

- Antivirus und Personal Firewalls als Basisschutz
- Application Control mit Whitelisting erlaubter Prozesse und Applikationen
- Hardening (Dokumentation von Sicherheitsrichtlinien, Risikobewertung, Optimierung von Einstellungen)
- Device & Port Control (Kontrolle der Client-Schnittstellen) und Data-Loss-Prevention-Module

>>> ENCRYPTION
Vertrauliche Daten müssen auch vertraulich bleiben. Um das sicherzustellen, kommen verschiedene Methoden zum Einsatz:

- Disc Encryption (Festplattenverschlüsselung v. a. für Notebooks)
- File Encryption (Dateiverschlüsselung zum Schutz vor unberechtigten Zugriffen)
- E-Mail Encryption (E-Mail-Verschlüsselung für externe und interne E-Mails)
- Data Encryption (Rights Management verschlüsselt Dokumente)

>>> CORPORATE ACCESS
Immer mehr Geräte, immer mehr Zugänge. Grund genug, sich mit der Verschlüsselung der Infrastruktur zu beschäftigen:

- Remote Access VPN (mobiler Zugriff auf Unternehmensressourcen)
- Network Access (Verbindungen via WLAN, UMTS, LAN)

>>> MOBILE SECURITY
Ein Arbeitsplatz muss auch mobil sicher sein. Unsere Lösungen sind:

- Native Mobile Security (Basisschutz für mobile Geräte mit Mobile Device Management)
- Container Mobile Security (vor allem für BYOD eine sichere Lösung: Unternehmensdaten werden in sichere ‚Container' auf dem mobilen Gerät synchronisiert und können diese nicht verlassen)
- Virtual Mobile Security (sicherste Variante, Daten bleiben im Unternehmen, sind durch Virtualisierung auf dem Gerät verfügbar und können remote bearbeitet werden)

DATACENTER SECURITY – VERFÜGBARKEIT, VERTRAULICHKEIT, INTEGRITÄT

Rechenzentrums- und Applikationsausfälle sind tabu! Denn sie kosten bares Geld. Es gilt also, die zentralen Ressourcen eines Unternehmens, seine Daten und die Prozesse, mit denen diese Daten nutzbar gemacht werden, im Datacenter sorgfältig abzusichern. Kurzum: Verfügbarkeit, Vertraulichkeit und Integrität der Daten und Systeme stehen allzeit im Mittelpunkt.

Um sich vor geschäftskritischen Ausfällen zu schützen, ist ein integriertes und ganzheitliches Sicherheitskonzept vonnöten. Und die Anforderungen an die IT-Sicherheit im Datacenter ändern sich gerade enorm: Durch den vermehrten Einsatz von Cloud-Lösungen, die zunehmende Konsolidierung und eine hohe Nachfrage nach Mandantentrennung werden Rechenzentren immer größer. Damit wird auch der Schutz von Daten und Prozessen im Datacenter komplexer. Die Rechenzentrumsinfrastruktur – Storage, Server, Backupsysteme – muss ebenso wirksam abgesichert werden wie Betriebssysteme, Middleware, Applikationen und die dazugehörigen Management- und Monitoring-Tools. Unabhängig von Größe, Komplexität und geografischer Verteilung.

Hinzu kommen branchenspezifische Logging- und Auditingvorgaben, beispielsweise von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

DATACENTER SECURITY – WAS GEHÖRT DAZU?

>>> STORAGE SECURITY
Datenzugriffe auf Speichersysteme müssen überwacht und die dort gelagerten Daten geschützt werden. Das geschieht mit:
- Access Monitoring (Überwachung der Datenzugriffe auf Storage-Systeme)
- Storage Encryption (Datenverschlüsselung und Schutz vor Verlust der Schlüssel)
- Malware Protection (effizienter Virenscan)

>>> DATABASE SECURITY
Zugriffe kontrollieren und Angriffe erkennen mithilfe von:
- Access Monitoring (Auditanforderungen für die Zugriffe auf Datenbanken ohne Performanceeinbußen gerecht werden)
- Database Firewall (Angriffe auf Applikationsebene erkennen und somit Angriffe auf Datenbankebene verhindern)

>>> SERVER SECURITY
Ob Basisschutz oder Lösungen für einen hohen Schutzbedarf – zum Einsatz kommen:
- Hardening (Server robuster machen und Angriffsfläche reduzieren)
- Malware Protection (Basisschutz: Virenschutz und Firewall)
- Application Control (proaktiver Schutz durch Whitelisting)

>>> SECURE VIRTUALIZATION
Virtuelle Umgebungen brauchen passende Sicherheitslösungen, beispielsweise:
- Firewalls (virtuelle Firewalls im Network- oder Hypervisor-Mode oder im Software Defined Network)
- Malware Protection (agentenbasierte oder agentenlose Lösungen)
- Access & Authorization (sichere Verwaltung mit Berechtigungs- und Administrationskonzepten)
- Compliance Management (Statusdokumentation für virtuelle Umgebungen integriert ins Management virtueller Systeme)

>>> WEBAPP SECURITY
Webanwendungen überprüfen und sicher machen, ohne Nutzer zu „nerven", geht mit:
- Web Application Firewall (HTTP-Verkehr auf Anwendungsebene schützen)
- Source Code Analysis (Schwachstellen in Webanwendungen durch definierten Software-Entwicklungsprozess eliminieren)
- Penetration Scanning (Überprüfung von Webanwendungen auf ihre Sicherheit)

>>> SHAREPOINT SECURITY
SharePoint als zentrale Webanwendung lässt sich effizient schützen mit:
- Access Governance (Berechtigungsmanagement und Access-Monitoring)
- Authentisierung (Zugriffsmöglichkeiten erweitern)
- Malware Protection (zusätzlicher Virenscan für SharePoint)
- SharePoint Web App Security (Schutzfilter und sichere SharePoint-Programmierung)
- Information Rights Management (automatische Verschlüsselung von Dokumenten aus SharePoint)

>>> SECURE DATASHARE
Der Austausch von Daten mit anderen Nutzern, Datenzugriff und Synchronisation von verschiedenen Geräten – zeitgemäßes Arbeiten benötigt zuverlässigen Schutz mit:
- Clientbasierter Verschlüsselung von DataShare-Lösungen aus der Cloud, auch für hohe Sicherheitsanforderungen

NETWORK SECURITY – INTELLIGENTER SCHUTZ FÜR DATENBAHNEN

Das Netzwerk ist der zentrale Nervenstrang der Unternehmens-IT. Und der muss intakt sein. Weil hier alle wichtigen Daten ständig unterwegs sind, ist die professionelle Absicherung Pflicht und die Basis aller Security-Konzepte. Schließlich entwickeln Angreifer ständig neue, fortschrittlichere Methoden, die es abzuwehren gilt.

Netzwerke sind ein attraktives Angriffsziel – das waren sie schon immer. Firewalling, Intrusion Prevention und sichere VPN-Verbindungen gehören deshalb zur Grundausstattung. Hinzu kommt, dass Trends wie Cloud Computing und Virtualisierung sowie die Verlagerung von Applikationen ins Web neue Verteidigungsmethoden erforderlich machen, um sich vor Angriffen zu schützen. So müssen die Protokolle HTTP und DNS, über die heute quasi alle Daten übertragen werden, gründlich analysiert werden. Eine gute Security muss erkennen, ob das, was über HTTP oder DNS läuft, erlaubt ist oder nicht.

SECURITY-ZONEN MIT ZUKUNFT

Nach wie vor ist aber Fakt: Ein Netzwerk lässt sich recht gut in verschiedene Bereiche unterteilen und abtrennen, beispielsweise mit verschiedenen Nutzerkreisen. Im Fall der Fälle sind mit der richtigen Ausrüstung die Auswirkungen durch den Einsatz von Security-Zonen also begrenzbar. Und hier tut sich noch einiges, denn statische Zonen waren gestern. In Zukunft werden Systeme mit Zoneneigenschaften versehen, die unabhängig vom Ort mitwandern. Gerade mit Blick auf Virtualisierung und Cloud Computing werden Zonenkonzepte auf diese Weise dynamischer, flexibler und sicherer. Dieser Trend wird sich übrigens durch IPv6 und Software Defined Networking weiter verstärken.

SECURE NETWORK – WAS GEHÖRT DAZU?

>>> BORDER CONTROL

Türsteher fürs Netzwerk – die Einlasskontrolle übernehmen:

- Next Generation Firewalling (Netzwerk-Zonenmodelle und User-/Applikations-Zuordnung)
- Intrusion Prevention (Schutz vor Angriffen auf Netzwerkebene)
- Content Security (Inhaltskontrolle für Web und E-Mail)
- APT Protection (Schutz vor zielgerichteten Angriffen und fortschrittlicher Malware)

>>> APPLICATION DELIVERY

Anwendungen müssen sicher bereitgestellt werden. Hierzu kommen zum Einsatz:

- Web Application Firewalling (HTTP-Verkehr auf Anwendungsebene schützen)
- Load Balancing (Skalierbarkeit und Verfügbarkeit, elastische Infrastrukturen)
- SSL Offloading (zentrale SSL-Verschlüsselung zur Entlastung der Webserver-Farmen)
- Reverse Proxy (Authentifizierungsinstanz für sichere Veröffentlichung von Webanwendungen)

>>> BASE SERVICES

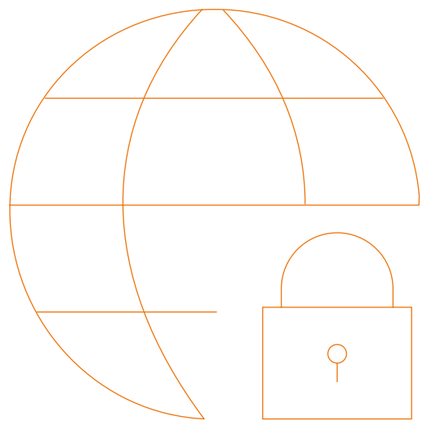
Wie überall muss die Basis stimmen. Im Secure Network sorgen dafür:

- DNS/DHCP (Management von IP-Adressen und Hostnamen)
- IPv6 Readiness (Anpassen der Security an neues Internetprotokoll IPv6)
- Network Authentification (Kontrolle des Netzwerkzugangs als zentrales Element einer Sicherheitsrichtlinie)

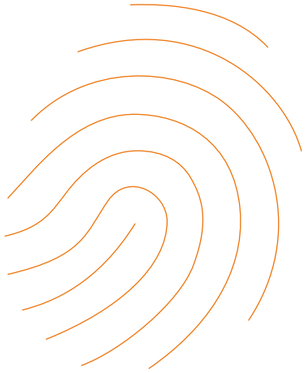
>>> TRAFFIC ENCRYPTION

Den Datenverkehr in eigenen und fremden Netzwerken sichern geht mit:

- Site to Site VPN (Verschlüsselung bei der Nutzung nicht vertrauenswürdiger Netzwerke)
- Remote Access VPN (Sicherer Netzwerkzugang für mobile Mitarbeiter)
- WAN Encryption (Verschlüsselung von WAN-Verbindungen zur Wahrung der Vertraulichkeit)



IDENTITY & ACCESS MANAGEMENT – ROLLEN UND RECHTE UNTER KONTROLLE



Komplexe Themen brauchen ein gutes Management – das gilt auch für Identitäten und Zugriffsrechte. Denn davon gibt es jede Menge: Jeder Mensch, jeder Computer, jede Applikation besitzt eine digitale Identität. Manchmal sogar mehrere. Und die haben unterschiedliche Rechte und wollen verwaltet werden. Führt das zwangsläufig ins Chaos?

Identitäten wie Sand am Meer gibt es in vielen Unternehmen. Jede muss mit Informationen zu Autorisierung und Authentisierung verknüpft sein und über ihren Lebenszyklus hinweg gemanagt werden. Klingt kompliziert. Ist es auch. Aber es gibt einen Ausweg: Damit Verzeichnisdienste nicht im Chaos enden, müssen Lösungen für das Identity & Access Management (IAM) her. Grundlage sind starke Authentisierungen, Public-Key-Infrastrukturen und Single-Sign-On für die Anwender. Ein gutes IAM definiert jederzeit, welche digitale Identität zu welcher natürlichen Identität gehört und auch, welche Rollen und Rechte diese hat.

(DIGITALE IDENTITÄT X (ANWENDUNG + GERÄT)) + COMPLIANCE = CHAOS?

Und es kommt noch besser, denn auch beim Thema Identitäten müssen definierte Richtlinien und Prozesse eingehalten werden, um die geforderte Compliance sicherzustellen. Wer sein IAM um ein Identity Governance Risk & Compliance Management (Identity GRC) ergänzt, hat hier bestens vorgesorgt. Soweit, so komplex. Aber immer noch nicht komplex genug. Denn ein Thema kommt gern zu kurz: die Rechte privilegierter Accounts, meistens Admin-Rechte. Ein gutes IAM muss sich auch diesem Thema widmen. So hilft IT Administration Control dabei, auch privilegierte Accounts mit weitreichenden Rechten sicher und effizient zu managen.

IDENTITY & ACCESS MANAGEMENT – WAS GEHÖRT DAZU?

>>> ACCESS MANAGEMENT

Wer hat wann, wie und worauf Zugriff? Das regeln:

- Privileged Account Management (administrative Accounts durch zentrales Passwortmanagement vor Missbrauch schützen)
- Strong Authentication (Authentisierung mit mehr als einem Passwort für Systeme mit höherem Schutzbedarf)
- Identity Federation (Verschlanken von Registrierungs- und Berechtigungsprozessen durch etablierte Vertrauensstellungen)
- Public Key Infrastructure (Zertifikate für diverse Einsatzzwecke, Basisinfrastruktur)

>>> PROVISIONING

Daten bereitstellen, Prozesse effizient abbilden – dabei unterstützen:

- Datenkonsolidierung (automatische Synchronisation von Personen-, Kommunikations- und Organisationsdaten ermöglichen)
- Process Automation (Automatisierung von Administrationsvorgängen)
- Self Services/IT Service Portal (Zugang zu IT-Services für Mitarbeiter)
- Password Management (Verwaltung der Passwörter für IT-Systeme durch Mitarbeiter)

>>> IDENTITY COMPLIANCE

Compliance-Anforderungen müssen erfüllt werden, beispielsweise mit:

- Kontrollsystemen (Regelwerk für Compliance-Anforderungen)
- Validation (Prüfung der Berechtigungen anhand des Compliance-Regelwerks)
- Role Management (Management von Berechtigungen erleichtern)
- Auditing/Reporting (Ergebnis der Prüfung darstellen, notwendige Korrekturen werden sichtbar)

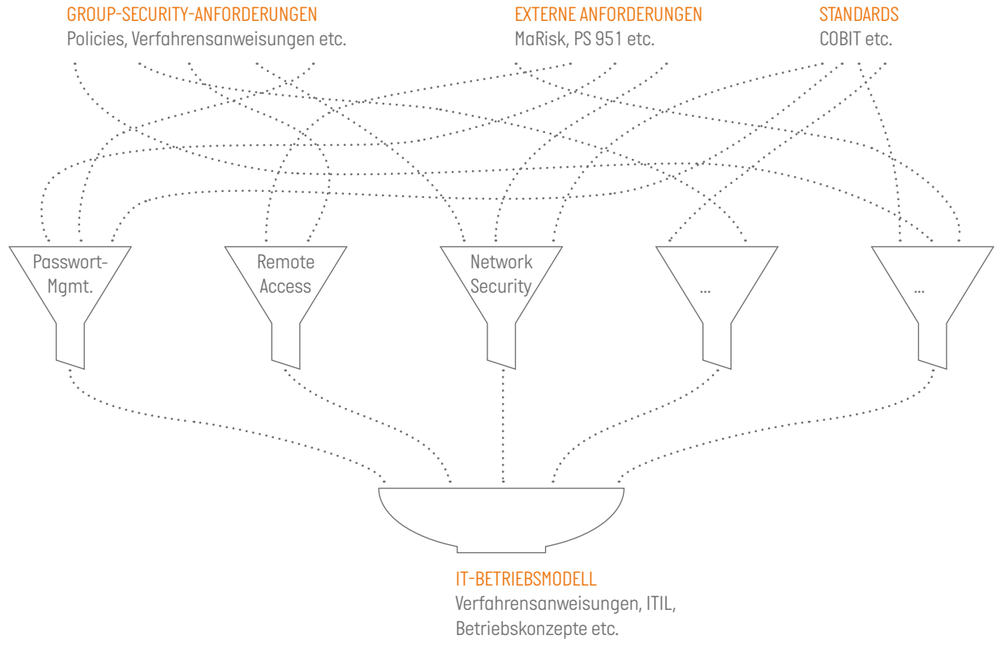
INFORMATION SECURITY MANAGEMENT – KLARHEIT BEI COMPLIANCE & CO.

Richtlinien für die IT-Sicherheit braucht jedes Unternehmen. Schon allein aus Compliance-Gründen. Wer aber definiert diese Richtlinien und wer sorgt dafür, dass diese auch umgesetzt werden? Der IT-Betrieb? Oder Corporate Governance?

Die Praxis hat ihre eigenen Regeln: Oft definiert die IT-Abteilung nach bestem Wissen und Gewissen ihre Anforderungen und setzt passende Security-Maßnahmen um. Gleichzeitig gilt es, externe Anforderungen aus Gesetzen wie dem Bundesdatenschutzgesetz zu beachten oder auch solche, die in der Governance-Abteilung definiert wurden. Aber passen beide Ansätze hundertprozentig zusammen und führen zu den gleichen Maßnahmen? Nicht unbedingt. Leider bleibt die Frage oft unbeantwortet, weil kein Abgleich stattfindet – die organisatorische Lücke scheint zu groß.

BRÜCKEN SCHLAGEN

Ausweglos? Mitnichten, denn ein ausgeklügeltes Information Security Management System (ISMS) kann diese Lücke schließen. Es steuert die gesamte Security und managt die Anforderungen – interne wie externe. Ein ISMS definiert Rollen, Prozesse, Verantwortlichkeiten und Richtlinien. Und es setzt diese vom Anforderungsmanagement bis in den IT-Betrieb hinein um – inklusive Aufbau- und Ablauforganisation. So werden organisatorische Lücken zwischen Soll und Ist sichtbar gemacht und können geschlossen werden. Und wer es perfekt machen will, lässt sein ISMS zertifizieren – nach ISO 27001 für Unternehmen oder dem BSI IT-Grundschutzkatalog für die Öffentliche Hand.



INFORMATION SECURITY MANAGEMENT – WAS GEHÖRT DAZU?

>>> PROCESSES AND METHODS

Beratung bei der methodischen Umsetzung eines Information Security Management Systems auf Basis von Standards wie ISO 27001

>>> CONTROL COMPLIANCE

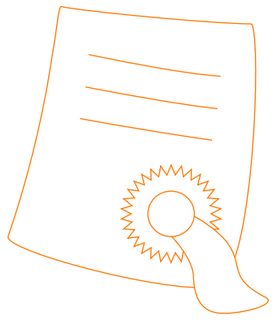
Compliance automatisieren – wir haben unsere eigene, praxiserprobte Methode

- Teilaspekt definieren, der automatisiert werden kann
- Komplexe regulative Anforderungen mit bereits vorhandenen Schutzmaßnahmen abgleichen
- Compliance-konforme Umsetzung von Anforderungen automatisiert nachweisen

>>> AUTOMATION

Datenbank-Tool statt Excel

- ISMS-Prozesse aus der Lösungsgruppe „Processes and Methods" sind automatisierbar.
- Das geschieht, indem die erforderlichen Daten in einem Datenbank-basierten Tool abgebildet werden – in den meisten Fällen wird hiermit Excel abgelöst.



CYBER DEFENSE – ANGRIFFE SCHNELL ERKENNEN UND REAGIEREN

Sind wir mal ehrlich: Erfolgreiche Angriffe auf die Unternehmens-IT lassen sich heute nicht mehr verhindern. Umso wichtiger ist es, Angriffe möglichst früh zu erkennen. Und richtig zu reagieren.

IT-Sicherheit ist vielschichtig geworden – und damit unübersichtlich. Um alles im Blick zu behalten, helfen ein zentrales Management und ein automatisierter Rundumblick auf die IT-Security. So kann Schaden abgewendet werden, bevor er entsteht. Aber präventive Maßnahmen, so gut sie auch sein mögen, schließen nicht zwangsläufig erfolgreiche Angriffe aus. Das Tückische daran: IT-Sicherheitsvorfälle werden oft monatelang nicht entdeckt.

DAS SCOTLAND YARD DER IT-SICHERHEIT

Um das Schlimmste zu verhindern, müssen erfolgreiche Angriffe zeitnah und effizient erkannt, Ursachen ermittelt und nachhaltig behoben werden. Dazu braucht es verlässliche detektive und reaktive Fähigkeiten. Gar nicht so einfach? Doch! Mit einem Security Information & Event Management (SIEM), am besten direkt integriert in ein Security Operation Center (SOC): Hier laufen sämtliche Security-relevanten Informationsquellen zentral an einer Stelle zusammen, werden Spuren gesucht, Informationen ausgewertet und geeignete Maßnahmen eingeleitet – ein intelligentes Zusammenspiel von Technologien, Prozessen und Menschen. Darf es noch ein bisschen proaktiver sein? Mit einem Cyber Defense Center erreichen Sie die nächste Stufe. Die Kombination forensischer Fertigkeiten und die Auswertung neuer Erkenntnisse sorgen für eine noch bessere Prävention, indem Angriffe noch früher erkannt werden.

CYBER DEFENSE – WAS GEHÖRT DAZU?

>>> SOC ORGANIZATION

Damit ein Security Operation Center (SOC) funktioniert, muss es gut aufgestellt sein und sich in die Organisation einfügen. Zu einer Prozess- und Organisationsberatung gehören:

- Implementieren von Prozessen (u. a. Security Incident Response, Eskalations- und Meldeverfahren, Betriebsprozesse, Dokumentationsvorlagen)
- Definition und Beschreibung von Rollen (z. B. Analyst, Incident Manager, Forensiker)
- Cyber Defense Reporting (Integration in vorhandene Reporting-Werkzeuge, IT-GRC-Schnittstellen, KPI-Definition)
- Interfaces (Definition und Dokumentation von Schnittstellen in andere Bereiche, z. B. Krisenmanagement, IT-Betriebsabteilungen, Corporate Security, oder nach extern)

>>> SIEM & ANALYTICS

Ein Security Information & Event Management (SIEM) analysiert Logdaten und Events und kann dadurch Unregelmäßigkeiten und Angriffe aufspüren. Das macht die Abwehr robuster und schlagkräftiger. Dazu kombinieren moderne SIEM-Lösungen drei verschiedene Aspekte:

- SIM/Security Information Management (Logdaten langfristig und sicher speichern – inklusive Indexierung, Filterung und Reporting)
- SEM/Security Event Manager (zentrale Übersicht aller Security-Events – mit intelligenter Priorisierung von Incidents und automatischer Mustererkennung)
- Big Data Analytics (Data Mining und Mustererkennung, Visualisierung der Daten)

>>> VULNERABILITY MANAGEMENT

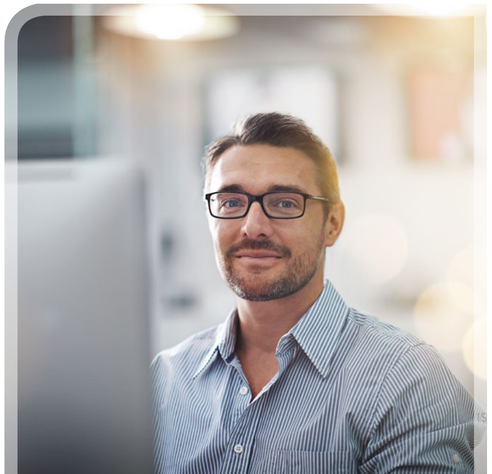
Jedes System hat Schwachstellen. Lokale oder über das Netzwerk erreichbare. Beide Formen gilt es mit internen oder externen Schwachstellen-Scans zu erkennen. Vulnerability Management unterstützt außerdem bei:

- Policy Compliance (Check auf Einhaltung der Systemstandards)
- PCI Compliance (Payment Card Industry: spezielle Regularien für Kreditkarten-Transaktionen erfüllen und automatisiert überprüfen)
- Malware Detection (Prüfung extern erreichbarer Systeme, ob durch sie Malware verbreitet wird)
- External Scanning (Sicherheitscheck der extern erreichbaren Systeme aus Angreifersicht)
- Web Application Scanning (Anwendungen auf Schwachstellen und Sicherheitslücken überprüfen)

>>> ATTACK DETECTION

Angriffe müssen erkannt werden, um reagieren zu können. Hierfür kommen zum Einsatz:

- Advanced Malware Detection (Verhaltens- und Kommunikationsanalysen zur Erkennung fortgeschrittener Schadsoftware)
- Traffic Data Analysis (Netzwerkverkehr und Metadaten auswerten, um Anomalien zu erkennen)
- Forensic Analysis (forensische Untersuchung von Systemen, Dateien und Netzwerkverkehr)
- Security Intelligence Collation (interne und externe Security-Informationen integrieren und aufbereiten)



IT-SECURITY – DEN ANWENDER IM FOKUS

IT-Sicherheit hat viele Facetten und ist das Fundament für den Unternehmenserfolg. Denn einerseits gibt es immer mehr Angriffe auf die IT-Systeme von Unternehmen. Andererseits erwarten Mitarbeiter und Kunden eine stabile, sichere und komfortable IT: in der täglichen Arbeit, bei der Kommunikation und sämtlichen Geschäftsprozessen – über alle Geräte und Kanäle hinweg. Aber damit nicht genug: Anwender wünschen sich außerdem, dass die IT noch benutzer- und informationszentrischer wird und sich ihren individuellen Bedürfnissen anpasst. Dass sie dabei auch sicher ist, wird einfach vorausgesetzt. Das heißt: Gute IT-Sicherheit begleitet und ermöglicht die Umsetzung neuer Anforderungen der Nutzer an die IT – und das ganz unaufdringlich und verlässlich im Gentleman-Style.

WIR VERSTEHEN ENTERPRISE-IT – UND DESHALB AUCH IT-SECURITY

Wie aber kommt man zu einer guten IT-Sicherheit, die all diese Aspekte vereint? Scheinbar passende Sicherheitslösungen einfach auf die bestehende IT „draufzupacken", ist keine Lösung. Vielmehr ist ein integrierter Blick auf die Gesamt-IT nötig. Und genau da kommen wir ins Spiel: Fehlt irgendwo die nötige Sicherheit, konzipieren wir sie direkt in Ihre Unternehmens-IT hinein statt nur obendrauf. Dabei kommt alles aus einer Hand: von der Beratung über Konzeption und Implementierung bis hin zu Betriebsunterstützung und Wartung. Wir arbeiten mit allen wichtigen Herstellern im Markt zusammen und stimmen uns intern mit den Experten anderer IT-Disziplinen auf kurzen Wegen ab. So stellen wir sicher, dass die Beratung nur das empfiehlt, was sich im Live-Betrieb auch umsetzen lässt. Versprochen.

COMPUTACENTER: IHR PARTNER – IHRE VORTEILE

- 15 Jahre Security-Erfahrung kombiniert mit umfassendem IT-Know-how
- Integrierte IT-Lösungen aus einer Hand
- Herstellerübergreifende, zertifizierte und langjährige Partnerschaften
- Praxistaugliche IT-Lösungen
- Realisierung von mehr als 120 Projekten pro Jahr
- IT-Trends fürs Business nutzbar machen
- Anforderungen der Mitarbeiter an Geräte und Prozesse sicher gestalten
- Abdeckung des gesamten IT-Security-Lebenszyklus

Enabling users and their business

Computacenter ist Europas führender herstellerübergreifender Dienstleister für eine Informationstechnologie, die Anwender und deren Geschäft erfolgreich macht. Wir beraten Organisationen hinsichtlich ihrer IT-Strategie, implementieren die am besten geeigneten Technologien, optimieren ihre Performance oder managen die IT-Infrastruktur unserer Kunden.

Verwurzelt in europäischen Kernländern verbindet Computacenter globale Reichweite mit lokaler Kompetenz.

Computacenter

Computacenter AG & Co. oHG
Europaring 34–40, 50170 Kerpen

computacenter.de
+49 (0)2273 5970