www.pwc.de

Cyber Managed Services im Einsatz

Wann und wie Organisationen von gemanagter IT-Security profitieren

pwc

Inhaltsverzeichnis

„Unternehmen sind mit ständig neuen Cyberbedrohungen durch hochprofessionell agierende Akteure konfrontiert. Gleichzeitig müssen sie zunehmend strengere gesetzliche Vorgaben rund um IT-Sicherheit und Risikomanagement einhalten. Cyber Managed Services helfen dabei, die Resilienz nachhaltig zu erhöhen und die Compliance sicherzustellen. Wir skizzieren in diesem Whitepaper typische Einsatzszenarien und zeigen, welche Herausforderungen sich jeweils lösen lassen."

Moritz Anders
Partner

Einleitung

Die anhaltende Digitalisierung durchdringt immer mehr Bereiche unseres Lebens. Sie ermöglicht Unternehmen, ihre Produkte und Services zu innovieren und Abläufe effizienter zu gestalten – sei es durch die Vernetzung von Geräten im wachsenden „Internet der Dinge“ oder den völlig neuen Umgang mit Informationen und Inhalten durch die revolutionären Möglichkeiten generativer künstlicher Intelligenz. Je weiter die Digitalisierung jedoch voranschreitet, desto mehr Tore öffnen sich potenziell für cyberkriminelle Gruppen. Ohne angemessene IT-Sicherheit hängt nicht nur die digitale Dividende in der Schwebe. Erfolgreiche Cyberangriffe führen zu Betriebseinschränkungen, immensen Kosten und Reputationsschäden. Sie bedrohen Unternehmen in ihrer Existenz.

Digitalisierung und IT-Sicherheit müssen Hand in Hand gehen

Laut dem Bericht des BSI zur Lage der IT-Sicherheit in Deutschland 2023 ist die Bedrohung im Cyberraum aktuell so hoch wie nie zuvor. Die Anzahl der täglich registrierten Schwachstellen in Softwareprodukten ist im Beobachtungszeitraum des Berichts gegenüber dem Vorjahr um 24 Prozent gestiegen. Tag für Tag werden durchschnittlich 250.000 neue Schadprogramm-Varianten bekannt.

Neben der anhaltenden Gefahr, dass Ransomware-Angriffe die IT in Geiselhaft nehmen, eskaliert die Lage zunehmend auch durch geopolitische Konflikte. Russische Hacktivismus-Angriffe und Cyberspionage sind in Deutschland längst an der Tagesordnung. Nicht umsonst sehen laut dem Global Crisis and Resilience Survey 2023 von PwC 89 Prozent der Entscheider:innen Resilienz als strategische Priorität.

Zunehmend striktere regulatorische Vorgaben erhöhen den Compliance-Druck

Dass sich die Bedrohungslage seit Jahren zuspitzt, blieb auch dem Gesetzgeber nicht verborgen. Unternehmen sind mit zunehmend strikten Vorgaben konfrontiert und müssen bei Verstößen empfindliche Bußgelder zahlen. Zu den Regularien gehören Datenschutzbestimmungen und branchenübergreifende Regelwerke wie die NIS-2-Richtlinie, die das Gesamtniveau der Cybersicherheit in der EU steigern soll. Außerdem gibt es branchenspezifische Vorgaben wie den Digital Operational Resilience Act (DORA), der neue Regeln rund um Cybersicherheit für den Finanzsektor vorschreibt.

Cyber Managed Services ermöglichen die Auslagerung bestimmter Sicherheitsaufgaben

Um die gestiegenen Anforderungen an die Cybersicherheit angemessen zu adressieren, müssen Unternehmen ihre Cyberabwehr professionalisieren. Dabei ist es nicht immer sinnvoll oder möglich, alle nötigen Ressourcen intern aufzubauen und sämtliche Aufgaben aus eigener Kraft zu stemmen. In vielen Fällen ist es günstiger, verlässlicher und sicherer, bestimmte Funktionen auszulagern. Die Zusammenarbeit mit Dienstleistern gewinnt an Bedeutung.

Hier kommt das Modell „Cyber Managed Service“ ins Spiel, bei dem ein Managed Service Provider (MSP) ausgewählte Sicherheitsaufgaben übernimmt. Doch in welchen Fällen bietet sich dieses Modell besonders an? Wie funktioniert in der Praxis die Zusammenarbeit zwischen Auftraggeber und MSP? Welche Vorteile ergeben sich durch die Auslagerung? Antworten auf diese Fragen geben wir in den folgenden Kapiteln, in denen wir jeweils Einblicke in konkrete Einsatzszenarien geben.

Was sind Cyber Managed Services?

Cyber Managed Services adaptieren das Dienstleistungsmodell der Managed Services für den Bereich der IT-Sicherheit. Ein Managed Service Provider (MSP) übernimmt die Verantwortung für sicherheitsrelevante Funktionen oder Prozesse Aufgaben eines Unternehmens – sei es das Identitäts- und Zugriffsmanagement, die Risikobewertung, oder die Erkennung von und das Reagieren auf Bedrohungen. PwC setzt bei diesem Ansatz auf eine Kombination aus State-of-the-Art-Technologien und interdisziplinärem Fachwissen. Ein Kerngedanke besteht darin, die Aufgaben nicht nur zu übernehmen, sondern deren Abwicklung kontinuierlich zu verbessern.

A Neuaufbau der IT nach Umstrukturierung – Vermögensverwaltung errichtet IT in Rekordzeit

Der Use Case im Überblick

Ausgangssituation:
- Die Notwendigkeit, neue IT-Abteilungen und -Fähigkeiten aufzubauen aus einer Großbank
- IT-Organisation muss für Gesellschaft mit mehr als 3.000 Mitarbeitenden neu etabliert werden

Herausforderungen:
- Hoher Zeitdruck für nahtlosen Übergang des Betriebs ohne Unterbrechungen
- Gewährleistung von Sicherheit in dynamischer Bedrohungslandschaft
- Sicherstellung der Compliance bei komplexer Regulatorik der Finanzindustrie
- Eingeschränkte Ressourcen und Expertise für nachhaltigen Betrieb

Eingesetzte Cyber Managed Services:
- Digital Identity
- Cyber Defense
- Cyber Risk

Vorteile:
- Unterstützung zur Behebung von Prüfungsfeststellungen
- Proaktive Gewährleistung der betrieblichen Compliance und Resilienz
- Erhöhte Resilienz durch hochqualifizierte Cyber-Expert:innen und strategische Allianzen
- Standardisiertes und effizientes Vorgehen durch Best Practices und Ausnutzung von Automatisierungspotenzialen

Der Neuaufbau der IT-Abteilungen und -Fähigkeiten war beschlossene Sache. Bald sollte die Vermögensverwaltung einer Großbank als eigenständige Einheit am Markt auftreten. Dieser Entscheid setzte eine Maschinerie in Gang, die auch den IT-Betrieb erfasste. Für über 3.000 Mitarbeitende musste eine komplett neue IT-Infrastruktur aufgesetzt werden.

Neue IT-Organisation unter Zeitdruck etablieren

Während der Aufbau einer IT-Organisation dieser Größe üblicherweise ein bis drei Jahre in Anspruch nimmt, sollte die Ausgliederung innerhalb weniger Monate vollzogen werden. Zwar lassen sich in so einer Situation unter Umständen bestimmte organisatorische Vorgaben der übergeordneten Organisation als Vorlage verstehen. Sie sind in der Praxis jedoch nicht mehr als eine Inspiration. Die tatsächliche Umsetzung bleibt eine vielschichtige individuelle Aufgabe des ausgegliederten Unternehmens. Sie reicht vom Entwurf einer Data Governance- und Datenschutzrichtlinie bis hin zur Konfiguration von Zugriffskontrollen.

Erschwerend trat in diesem konkreten Fall hinzu, dass die Vermögensverwaltung die hohen regulatorischen Vorgaben der Finanzindustrie einhalten muss. Dazu gehören Vorgaben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) wie die Bankaufsichtlichen Anforderungen an die IT (BAIT) und Mindestanforderungen an das Risikomanagement (MaRisk) sowie weitere Regularien der Europäischen Bankaufsichtsbehörde (EBA).

Auslagerung von Aufgaben der Cybersicherheit durch drei Managed Services

Schnell war klar: Eine angemessene Absicherung der neu aufzubauenden IT war aus eigener Kraft nicht möglich. Allein die richtigen Security-Spezialist:innen zu finden, war in so kurzer Zeit utopisch. Gleichzeitig wollte die Vermögensverwaltung aber nicht alles aus der Hand geben. So entschied man sich für einen Mittelweg: Das Unternehmen kümmert sich selbst um den Betrieb der wesentlichen Infrastruktur und greift auf drei Managed Services von PwC zurück, um die Sicherheit und die Einhaltung der Compliance-Vorgaben zu gewährleisten.

Der Cyber Managed Service Digital Identity deckt die Bereiche Identity and Access Management (IAM) und Priviledged Access Management (PAM) ab – zwei wesentliche Komponenten der Cybersicherheitsstrategie einer Organisation. Erstere verwaltet den Zugang für normale Nutzer und ihre täglichen Aktivitäten. Letztere kontrolliert privilegierte Nutzer, die Zugriff auf sensible Systeme und Daten haben. Der Managed Service Cyber Defense monitort potenzielle Incidents, analysiert Schwachstellen und stärkt die Cyberabwehr durch entsprechende Gegenmaßnahmen. Cyber Risk hilft dabei, Cyberbedrohungen und damit verbundene Risiken kontinuierlich zu analysieren und zu mindern.

Die Einführung der Cyber Managed Services erfolgte schrittweise. Eine wesentliche Herausforderung dabei lag in den unterschiedlichen Entwicklungsstadien der zugrunde liegenden Umgebungen. Einige waren bereits vollständig implementiert, andere befanden sich noch im Aufbau. Die Arbeitsteilung zwischen Auftraggeber und MSP erforderte eine sorgfältige Abstimmung. Dank der engen Zusammenarbeit der internen Teams mit den Teams von PwC verlief die Übergabe reibungslos.

Abgesichert gegen Cyberangriffe und gut aufgestellt für Audits

Nach der erfolgreichen Übergabe übernahm PwC die vollständige Durchführung der vereinbarten Funktionen. Neben der kompletten operativen Abwicklung fanden weiterhin Beratung und Austausch auf strategischer und taktischer Ebene statt. So wird beispielsweise laufend überprüft, ob aktuelle Best Practices angewendet werden.

In enger Abstimmung werden die Prozesse kontinuierlich weiterentwickelt, um Cyberangriffen effektiv vorzubeugen, die Resilienz zu erhöhen und alle Compliance-Anforderungen zu erfüllen – und das vor dem Hintergrund einer sich ständig verändernden Bedrohungslage und einer anhaltenden Dynamik in der Gesetzgebung. Die Vermögensverwaltung profitiert dadurch unter anderem von einer hochentwickelten Cyberabwehr rund um die Uhr, ohne ein eigenes 12-köpfiges Team für ein entsprechendes Security Operations Center aufbauen zu müssen.

Wie wir das Einsatzszenario bewerten

Umstrukturierungen stellen die IT vor enorme Herausforderungen. Gerade in den Parallelwelten von Übergangsphasen ist Chaos vorprogrammiert. Und das ist genau die Situation, die Hacker lieben und gezielt ausnutzen. Bei knappen Ressourcen und hohem Zeitdruck bieten Cyber Managed Services hier einen Ausweg. Sie helfen dabei, die Cyberrisiken zu minimieren, die neue Organisation von Anfang an resilient aufzustellen und regulatorische Anforderungen sicher einzuhalten.

Die Ausgestaltung der Services kann dabei sehr unterschiedlich sein. Im beschriebenen Fall verantwortet der Auftraggeber die Infrastruktur. Dies ist eher typisch für Großunternehmen. Im Mittelstand empfiehlt sich häufig auch das Auslagern der Infrastruktur, wenn ein sicherer Betrieb mit den eigenen Ressourcen nicht gewährleistet werden kann. Grundsätzlich lassen sich unterschiedliche Anforderungen über individuelle Serviceverträge mit klar definierten SLAs und KPIs abbilden.

B Professionalisierung der IT-Security – Maschinenbauer reaktiviert gehackte IT-Umgebung

Der Use Case im Überblick

Ausgangssituation:

- Ransomware-Angriff zwingt Maschinenbaubetrieb zur Stilllegung seiner IT-Infrastruktur
- Neues Aufsetzen der IT-Umgebung ist in vertretbarer Zeit nicht möglich wegen Legacy-Systemen in heterogener, global verteilter IT-Landschaft
- Umgebung soll mit angemessenen Schutz- und Kontrollmaßnahmen schrittweise wiederhergestellt werden

Herausforderungen:

- Weiteren Cyber Incidents muss effektiv vorgebeugt werden
- Verfügbare eigene IT-Ressourcen sind knapp
- Asset Management ist nicht implementiert – es gibt keine Configuration Management Database
- Schnelle Wiederherstellung der IT-Umgebung ist geschäftskritisch

Eingesetzte Cyber Managed Services:

- Cyber Defense

Vorteile:

- 24x7-Monitoring durch Security Operations Center während Wiederherstellung der angegriffenen Umgebung und darüber hinaus
- Überwachung und Analyse von Sicherheitswarnungen; Identifizierung von möglichen Vorfällen
- Schnelle Reaktion durch 100%ige Triage-Automatisierung und integrierte Bedrohungsanalyse
- Empfehlungen für eine nachhaltig verbesserte Cyber-Hygiene

Als die IT-Abteilung bemerkte, dass sie sich einen Ransomware-Trojaner eingefangen hatte, zog sie die Notbremse. Die gesamte IT-Landschaft des Unternehmens – ein mittelständischer, international tätiger Maschinenbauer – wurde heruntergefahren. Eine Verschlüsselung der Systeme – und hoffentlich auch ein Abfluss sensibler Daten – konnte gerade noch verhindert werden.

Dennoch war das gesamte Netzwerk down. Die Auswirkungen auf den Betrieb waren massiv. Die Produktion wurde eingeschränkt. Mitarbeitende griffen zu Stift und Papier, waren aber nur bedingt arbeitsfähig. Die gesamte Kommunikation kam zum Erliegen und musste über alternative Kanäle wie private Messenger-Dienste abgewickelt werden.

Schrittweiser Wiederaufbau mit externer Sicherheitslösung

Die ersten Überlegungen zur Reaktivierung der IT-Landschaft gingen von einem kompletten Neubau aus. Schließlich war nicht genau bekannt, welche Teile des Netzwerks kompromittiert waren. Ebenso ungewiss war, inwieweit die Backups betroffen waren. Als den Verantwortlichen jedoch klar wurde, dass ein Neuaufbau Monate dauern würde und einige Legacy-Systeme kaum sinnvoll nachgebaut werden konnten, formte sich ein neuer Plan.

In Zusammenarbeit mit dem Incident Response Team von PwC wurde ein Lösungsansatz erarbeitet, der eine schrittweise Reaktivierung und Überprüfung der einzelnen Systeme ermöglichte. Die IT-Landschaft wurde hermetisch abgeriegelt, um dann die einzelnen hochgefahrenen Systeme systematisch zu analysieren und bei erkannten Problemen unter Quarantäne zu stellen.

Das Vorgehensmodell ist vergleichbar mit der Idee, von außen sämtliche Fenster und Türen eines Hauses zu verriegeln, in dem sich ein Dieb aufhält. Und dann im Inneren sukzessive einzelne Räume zu öffnen, um den Dieb zu stellen. Auf den einzelnen Systemen wurden dafür Agenten installiert, die das jeweilige System und seine Netzwerkumgebung überwachen. Die gesammelten Daten fließen an eine zentrale Softwarelösung und werden dort ausgewertet.

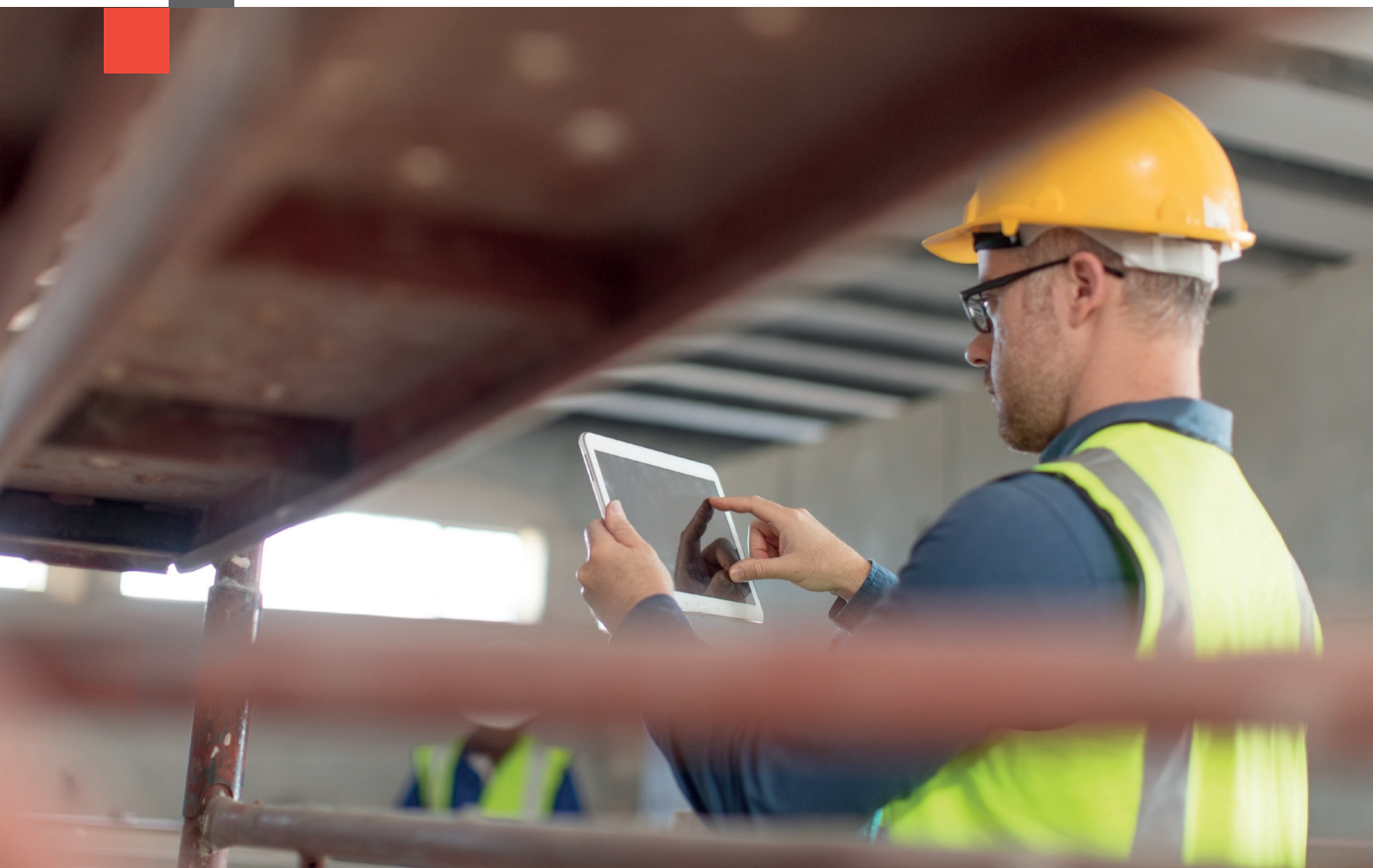
Security Operation Center mit 24x7-Monitoring
Um die IT-Sicherheit des Maschinenbaubetriebs während des Wiederaufbaus und darüber hinaus zu gewährleisten, setzte das Unternehmen auf den Managed Service Cyber Defense von PwC. Ein rund um die Uhr besetztes Security Operations Center (SOC) überwacht seitdem kontinuierlich die Umgebung. Pro Woche treten 300 bis 500 Alarme auf, die analysiert und nach ihrer Kritikalität eingestuft werden. Falls Handlungsbedarf besteht, wird das Unternehmen unmittelbar benachrichtigt.

Während des Wiederaufbaus und des kontinuierlichen Monitorings stellte sich heraus, dass das Unternehmen wichtige Sicherheitslösungen nicht implementiert hatte. So fehlte beispielsweise ein Asset Management. Es gab schlichtweg keine systematische Übersicht, welche Geräte und Systeme im Unternehmen überhaupt im Umlauf waren. Daraus ergab sich ein hoher Abstimmungsbedarf, aber auch die Chance für das Unternehmen, erkannte Lücken zu schließen und sich besser aufzustellen.

Wie wir das Einsatzszenario bewerten

Auch mit den besten Sicherheitsvorkehrungen lässt sich ein Cyber Incident nicht hundertprozentig ausschließen. In der Praxis sind Incidents aber häufig auf Versäumnisse zurückzuführen – seien es falsche Konfigurationen, veraltete Software oder gänzlich fehlende Sicherheitslösungen. Hacker gehen meist den Weg des geringsten Widerstands. Gerade für mittelständische Unternehmen wird es aufgrund des hochprofessionellen Vorgehens cyberkrimineller Gruppen zunehmend schwerer, sich aus eigener Kraft angemessen abzusichern.

Managed Services bieten Möglichkeiten, um die Cyber-Abwehr zu härten. Idealerweise geschieht dies vor einem Incident, um die Risiken zu senken. Doch auch in den Nachwehen eines Vorfalls im Zuge des Aufbaus einer neuen Sicherheitsorganisation ist externe Unterstützung sehr sinnvoll. Mit Managed Services können Unternehmen die Reife ihrer Sicherheitsvorkehrungen kosteneffizient erhöhen, ohne gleich ein eigenes Security Operations Center aufbauen zu müssen.



C Einhaltung regulatorischer Vorgaben – Versicherungskonzern adressiert DORA-Compliance

Der Use Case im Überblick

Ausgangssituation:
- Versicherungskonzern ist von der DORA-Finanzregulierung betroffen
- Neue Cybersicherheits- und operationale Widerstandsfähigkeitsmaßnahmen müssen implementiert werden

Herausforderungen:
- Interne Teams sind in wichtigen Digitalisierungsprojekten gebunden
- Mangelnde Expertise für eine sichere Umsetzung und Prüfung der verpflichtenden Maßnahmen
- Zeitdruck durch näher rückendes Anwendungsdatum der Regulierung

Eingesetzte Cyber Managed Services:
- Cyber Defense
- Cyber Risk

Vorteile:
- Entlastung der internen IT, die sich auf strategisch wichtige Digitalvorhaben fokussiert
- Klar dokumentierte und revisionssichere Prozesse zum Sicherstellen der DORA-Compliance
- Schutz vor Sanktionen durch nachweisbare Einhaltung der regulatorischen Vorgaben
- Einsatz von Best Practices für Schutz vor Cyberangriffen und erhöhte Resilienz

Neue gesetzliche Vorgaben kommen selten überraschend. Wer die regulatorischen Entwicklungen verfolgt, kann Neuerungen frühzeitig antizipieren. Nichtsdestotrotz können in der Zeit, in der die Umsetzung ansteht, mangelnde Ressourcen die Implementierung nötiger Maßnahmen behindern. Genau so erging es einem Versicherungskonzern mit der DORA-Finanzregulierung.

DORA verschärft Vorgaben für Cybersicherheit und operationale Widerstandsfähigkeit

Mit dem Digital Operational Resilience Act (DORA) hat die Europäische Kommission einen neuen gesetzlichen Rahmen geschaffen, der die operationale Widerstandsfähigkeit des Finanzsektors der EU stärken soll. Er richtet sich an ein breites Spektrum an Organisationen der Finanzindustrie und verpflichtet sie, eine Reihe von Maßnahmen rund um die Cybersicherheit und die operationale Resilienz zu implementieren, um Cyberangriffe effektiv abzuwehren und Störungen zu bewältigen.

In Deutschland sind mehr als 3.600 Unternehmen von DORA betroffen, darunter Kredit- und Zahlungsinstitute, Wertpapierfirmen, Handelsplätze, Versicherungs- und Rückversicherungsunternehmen, Ratingagenturen und IKT-Dienstleister. Beschlossen wurde das Regelwerk bereits am 14. Dezember 2022 vom Europäischen Parlament und Europäischen Rat. In Kraft getreten ist es am 17. Januar 2024 und die Anwendung greift ab dem 17. Januar 2025. In Deutschland wird DORA bzw. die EU-Verordnung 2022/2554 durch das Finanzmarktdigitalisierungsgesetz (FinmadiG) in nationales Recht umgesetzt.

Analyse der Anforderungen offenbart Handlungsbedarf

Kurz nachdem DORA in Kraft getreten ist, hat der Versicherungskonzern eine interne Taskforce gebildet, um die neuen Anforderungen zu verstehen und die Umsetzung der nötigen Maßnahmen zu planen. Die gute Nachricht: Nicht alle Vorgaben waren neu. So entsprachen einige Anforderungen an das Risikomanagement zum Beispiel den Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) der BaFin. Die Ausgangssituation war gut. Nichtsdestotrotz mussten zahlreiche ergänzende Maßnahmen implementiert werden – sowohl im Risikomanagement als auch bei der Behandlung von Cybervorfällen und dem geforderten „Threat-led Penetration Testing“.

Bei der Umsetzungsplanung zeigt sich schnell, dass Ressourcen fehlten. Die IT-Abteilung war stark ausgelastet und in strategisch wichtigen Digitalisierungsprojekten gebunden. Eine Neufokussierung auf DORA hätte dort zu massiven Verzögerungen geführt. Gleichzeitig war die Personaldecke sehr dünn besetzt, was die nötige Expertise im Bereich der IT-Sicherheit anging.

Cyber Managed Services unterstützen Einhaltung regulatorischer Vorgaben

Der Versicherungskonzern entschied sich dazu, die bestehenden Lücken zur Abdeckung der DORA-Anforderungen mit externer Hilfe zu füllen. Mit den Managed Services Cyber Risk und Cyber Defense von PwC werden die Vorgaben rechtssicher umgesetzt. Grundlage dafür sind die technischen Regulierungs- und Implementierungsstandards sowie Leitlinien, welche die Anwendung von DORA konkretisieren. Sie werden festgelegt durch die EU-Wertpapier- und die EU-Banken-aufsichtsbehörde sowie die Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung.

Der Versicherungskonzern kommt damit der Verpflichtung nach, IKT-Vorfälle sorgfältig zu managen und die eingesetzten Informations- und Kommunikations-technologien intensiv zu prüfen. So erhält das Unternehmen beispielsweise im Rahmen des Services Cyber Defense eine Übersicht der Vorfälle, die nach den vorgegebenen Kriterien von DORA klassifiziert sind. Das Unternehmen weiß dadurch genau, welche Vorfälle der BaFin als Aufsichtsbehörde gemeldet werden müssen und kann somit seine Berichtspflichten erfüllen.

Wie wir das Einsatzszenario bewerten

Bei vielen Unternehmen gibt es noch eklatante Lücken, was die Umsetzung von Maßnahmen der Cybersicherheit und des Risikomanagements durch regulatorische Vorgaben betrifft. Häufig sind zwar die nötigen Management-Systeme implementiert, aber die tatsächlichen Maßnahmen nur unzureichend umgesetzt. Daraus entstehen immense Risiken. Einerseits ist das Level an Sicherheit, das die Maßnahmen gewährleisten sollen, nicht gegeben. Andererseits drohen Sanktionen und Bußgelder, wenn die implementierten Verfahren den Prüfungen der Aufsichtsbehörden nicht standhalten.

Cyber Managed Services bieten hier die Möglichkeit, sowohl eine rechtskonforme Umsetzung der Maß-nahmen zu gewährleisten als auch die Resilienz der Organisation durch bewährte operative Maßnahmen nachhaltig zu erhöhen.

Wie wir Sie unterstützen

PwC gehört zu den führenden Cybersicherheitsberatern Europas. Durch unser umfangreiches Service-Portfolio im Bereich Cyber Security bieten wir viele unserer Dienstleistungen auch als Managed Service an.

Die Managed Security Services von PwC helfen Ihnen, Ihre Ziele schneller zu erreichen, indem sie viel mehr bieten als nur Outsourcing. Wir bringen die Fähigkeiten, das Know-how und die Leidenschaft unserer Mitarbeiter ein, um Ihre Geschäftsfunktionen von Anfang bis Ende zu betreiben, und arbeiten partnerschaftlich mit Ihnen und Ihren Teams zusammen.

Dabei setzen wir unter anderem auf ein Netzwerk von über 30 Technologiepartnern und kombinieren bewährte branchenspezifischen Lösungen mit maßgeschneiderten selbstentwickelten Technologien. Das Wichtigste: Wir wissen, wie wir Ihre Mitarbeitenden und Ihre aktuelle Betriebsumgebung nahtlos integrieren können, damit Sie schnell von den Ergebnissen profitieren.

Alle Cyber Managed Services auf einen Blick

Unser ergebnis- und best-practice-basierter Ansatz führt zu Kontrolleffektivität, Prozessoptimierung und Erfüllung von Compliance-Anforderungen.

Managed Digital Identity

Dienstleistung, die auf die Gestaltung und Implementierung eines Governance-Rahmenwerks, das digitale Identitäten innerhalb einer Organisation überwacht und verwaltet.

- Identity Governance
- Privileged Access

Managed Cyber Defense

Dienstleistungen, die helfen, Sicherheitsdaten, Ereignisse und Warnungen durch kontinuierliche Bewertung, Analysen und Automatisierung zu identifizieren und darauf zu reagieren.

- Threat Detection & Response
- Vulnerability Management
- High-Volume Testing
- Threat Intelligence
- Forensics and Analytics

Managed Cyber Risk

Dienstleistung, die Identifizierung, Analyse und Bewertung potenzieller Cyber-Bedrohungen und -Risiken fokussieren.

- Risk Assessment
- Risk Reporting
- Data-Trust-as-a-Service

Managed Cloud Security

Dienstleistungen, die Kunden helfen, digitale Identitätsrisiken proaktiv durch den Identitätslebenszyklus zu managen. Dies umfasst Risiken im Zusammenhang mit Unternehmens-, Verbraucher- und privilegierten Identitäten.

- Cloud security Posture
- Cloud Identity Entitlement Management
- Attack Surface Management

Managed Digital Identity

Identity Governance
Entwurf und die Implementierung eines Governance-Rahmens, der digitale Identitäten innerhalb einer Organisation überwacht und verwaltet

Priviledged Access
Sicherung, Kontrolle, Verwaltung und Überwachung privilegierter Zugänge zu kritischen Systemen. Unterstützt das Unternehmen dabei, Datenschutzverletzungen zu minimieren und vertrauliche Daten zu schützen

Managed Cyber Defense

Detection & Response
Verwaltet die Überwachung, Erkennung und Reaktion auf laufende oder potenzielle Vorfälle

Vulnerability Management
Management von Schwachstellen durch Ermittlung von Sicherheitslücken und Anwendung von Gegenmaßnahmen.

High-Volume Testing
Validierung und Analyse der Auswirkungen von Schwachstellen

Forensics & Analytics
Zusammenstellung von Daten für forensische Analysen und die Sammlung von Beweisen

Managed Cyber Risk

Risk Assessment
Identifizierung, Analyse und Bewertung potenzieller Cyber-Bedrohungen und -Risiken.

Risk Reporting
Systematische Analyse und Bereitstellung wesentlicher Informationen für das Management und die Abschwächung von Risiken

Data-Trust-as-Service
Gewährleistet die Sicherheit, Zuverlässigkeit und Konformität der Daten eines Unternehmens durch verschiedene Schutzmaßnahmen

Managed Cloud Security

Cloud Security Posture
Maßnahmen wie Zugangskontrollen, Datenverschlüsselung, Netzsicherheit usw.

Cloud Identity Entitlement Management
Verwaltung von Identitäten und Berechtigungen in Cloud-Umgebungen

Attack Surface Management
Analyse und Reduzierung der Angriffsfläche und der potenziellen Auswirkungen

Ihre Ansprechpersonen

Moritz Anders
Partner
Tel.: +49 1515 5455621
moritz.anders@pwc.com

Joshua Khosa
Senior Manager
Tel.: +49 1514 4254179
joshua.khosa@pwc.com

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen unseren Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expert:innennetzwerks in 151 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC Deutschland. Mehr als 14.000 engagierte Menschen an 20 Standorten. Rund 2,93 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

© Juli 2024 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. Alle Rechte vorbehalten.
„PwC“ bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.