Rödl & Partner

CYBERSECURITY

1. CYBERSECURITY-RESILIENZ IN DER OPERATIONAL TECHNOLOGY (OT)
2. INFORMATIONSSICHERHEIT UND DATENSCHUTZ ALS MANAGEMENTSYSTEM
3. VOM IT-NOTFALLKONZEPT BIS ZUM UMFASSENDEN BUSINESS CONTINUITY MANAGEMENT
4. EIN CYBERVORFALL: ZUSTÄNDIGKEITEN, PROZESSE & INSTRUMENTE RECHTZEITIG VORHER KLÄREN

Wir dürfen in die einzelnen Punkte eintauchen, um die Besonderheiten unseres Ansatzes zu verdeutlichen. Denn uns ist wichtig, dass wir den Bezug zu Pragmatismus und zur Wirtschaftlichkeit nicht verlieren. Dabei ist uns klar, dass Sicherheit auch bezahlbar bleiben muss.

ERSTENS

CYBERSECURITY-RESILIENZ IN DER OPERATIONAL TECHNOLOGY (OT)

Als Informationstechnologie (IT) wird gemeinhin die „typische“ Büro-IT-Systemlandschaft (Office, SAP, etc.) bezeichnet. Diese sind in den letzten Jahren zunehmend besser geschützt worden. Sicherheitspatches, Zugriffschutz, Segmentierung von Netzen und Systemen, Überwachungssysteme etc. zeigen zwar oftmals immer noch Lücken auf. Dennoch verzeichnen wir einen gewissen Reifegrad, welcher zuversichtlich stimmt.

Blickt man auf die IT-Systeme im operativen und produzierenden Umfeld – die sogenannte Operational Technology (OT) –, dann zeigen die Systeme bemerkenswerte Schwachstellen auf. Veraltete Softwarestände, schlecht gehärtete Einstellungen, eingebettet in unsicheren Umgebungen und vieles mehr machen es Angreifern leicht, diese Systeme zu kompromittieren und einen großen Schaden anzurichten.

Vor dem Hintergrund der stetig steigenden Komplexität (Internet of Things, integrierte Sensorik, neue Geschäftsmodelle), des Kunden- und Wachstumsdruck sowie dem stets vorhandenem Fachkräftemangel, erscheint die Situation nicht vorteilhaft.

Uns treibt hier an, dass wir unseren Kunden in einem kollaborativen Ansatz sowohl konzeptionell, als auch im laufenden Betrieb von Instrumenten für das Monitoren und das Updaten der OT ein verlässlicher Partner sein wollen.

- Strategie- und Konzeptberatung zur Absicherung der OT

- Betrieb einer cloudbasierten Management plattform für Monitoring, Wartung & Berichterstattung

- Unterstützung bei der Abwehr von OT-basierenden Angriffen

- Forensische Analysen im Falle von Sicherheitsvorfällen

Natürlich ist uns bewusst, dass Sicherheitslücken in der regulären IT auch weiterhin beachtet werden müssen. Sollte sich ebenso in dieser „typischen“ Büro-IT-Systemlandschaft ein Bedarf ergeben, so ist obiger Ansatz auch darauf anwendbar.

ZWEITENS

INFORMATIONSSICHERHEIT UND DATENSCHUTZ ALS MANAGEMENTSYSTEM

Sicherheit für Daten und Informationen sowie im Cyber-Umfeld setzt natürlich Technik voraus. Ohne Technik geht es nur, wenn man keine bedeutenden Daten und Informationen verarbeitet. Aber wo ist das heute oder in Zukunft noch gegeben?

Es ist vielmehr das Zusammenspiel von Technik und Organisation, welche auch wirksam dauerhaft Schutz bietet. Die Nutzung von Technik muss eingerahmt sein. Wichtige Prozesse und Verantwortlichkeiten sowie Steuerung und Überwachung – nicht nur in der IT – sind zu definieren und umzusetzen.

Für diesen Rahmen haben sich in den letzten Jahren gute Informationssicherheits-Managementsysteme (ISMS) entwickelt. Prominent ist hier die Normenreihe zur ISO / IEC 27001 ff zu nennen. Diese Reihe ist anerkannt und wird als Zertifizierungsgrundlage herangezogen bzw. von Dritten gerne und zunehmend als Nachweis für Sicherheit gefordert. Unternehmen, welche Dienste für Dritte anbieten und hierbei nicht unerheblich Daten verarbeiten unterwerfen sich oft dieser Norm und dem Audit zur Erlangung einer Zertifizierung. Der direkte Nutzen: Kundenaufträge und Wachstum!

Aber auch ohne dem Ziel einer Zertifizierung ist es ratsam, sich diesen Managementsystemen zuzuwenden. Beinhalten sie doch einen erheblichen Umfang an Erfahrung und das zugrundliegende Managementsystem entlastet – haftungstechnisch aber auch arbeitstechnisch.

Neben der Normenreihe ISO / IEC 27001 haben sich noch weitere, durchaus auch einfachere Systeme herausgebildet. Zu nennen ist hier CISIS12®, welche Informationssicherheit in zwölf Schritten ermöglicht. Auch hier ist eine Zertifizierung möglich, aber nicht nötig.

CISIS12® unterscheidet sich im Wesentlichen im Umfang der Anforderungen und teilweise auch in Bezug auf einen pragmatischeren Ansatz. In beiden Fällen lassen sich die Anforderungen in Bezug auf ein Datenschutzmanagementsystem gut integrieren bzw. erweitern. Unser Leistungsportfolio bezieht sich hierbei auf:

- Kurzcheck in Bezug auf einen ISMS-Reifegrad

- Strategieberatung in Bezug auf das zu verwendende Framework, den Anwendungsbe reich (Scope) sowie der schrittweisen Einführung

- Projektsteuerung und Coaching im Umfeld einer Einführung von ISO / IEC 27001ff oder CISIS12®

- Planung und Umsetzung von technischen und organisatorischen Sicherheitsmaßnahmen

- Vorbereitung auf eine potenzielle Zertifizierung sowie Begleitung

- Integration bzw. Erweiterung um datenschutzspezifische zusätzliche Anforderungen

Unabhängig von einer potenziellen Zertifizierung ist es heute nur jeder Geschäftsleitung angeraten, sich solcher ISMS – Elemente zu bedienen. Vielleicht auch schrittweise und bewusst in Teilen und wachsend.

Zu diesem Zweck bieten wir regelmäßig auch kostenfreie Orientierungs-Webinare an. Falls Interesse besteht, laden wir Sie gerne hierzu ein.

DRITTENS

VOM IT-NOTFALLKONZEPT BIS ZUM UMFASSENDEN BUSINESS CONTINUITY MANAGEMENT

Es ist nicht mehr zu übersehen. Laufend erfahren wir über die Nachrichten von der Zunahme von Vorfällen in Richtung Naturkatastrophen (Überflutungen in sonst ruhigen Gegenden, Erdbeben, Flächenbrände etc.), Lieferkettenproblematik (Mangel an Rohstoffen, Unterbrechung der Lieferkette, Ausfall von Personal, etc.), menschlichen Versagen (Fehlbedienung, fehlende QS, etc.) und Cyberkriminalität in den vielfältigsten Facetten. Potenzielle Ursachen wie Innentäter (bewusste Herbeiführung von Schäden, etc.) und Ausfälle in der Hardware (Netzteil defekt etc.) schließen sich nahtlos an.

Nicht für jedes Gefahrenszenario kann in einem Unternehmen zu hundert Prozent Vorsorge zur Vermeidung oder Abwehr betrieben werden. Oftmals ist es dennoch eine Abwägung zwischen Kosten der Vorsorge, Eintrittswahrscheinlichkeit und Schadensumfang.

Und für solche Situationen sind Pläne aufzustellen, welche einen Wiederanlauf und eine Wiederherstellung in einem tolerierbaren Zeitraum ermöglichen. Liegt im „Scope“ nur die IT, dann spricht man von einem IT-Notfallplan bzw. IT-Service Continuity Managementsystem (IT-SCMS). Ist auch das Business einbezogen, so bezieht sich das auf ein Business Continuity Managementsystem (BCMS).
Durch unsere Erfahrungen im Betrieb unserer eigenen Daten- und Rechenzentren sowie über die Beratung von vielen Kunden verfügen wir derzeit über eine wertvolle Grundlage zum Aufbau solcher Systeme. Dies umfasst:

- Strategieberatung zur Planung und Organisation von BCMS bzw. IT-SCMS (auch international)

- Projektsteuerung und Überwachung

- Aufbau von Konzernregelungen, Handbüchern und Vorlagen

- Auswahl von technischen Unterstützungs werkzeugen (Benachrichtigung, Kommunikation im Notfall)

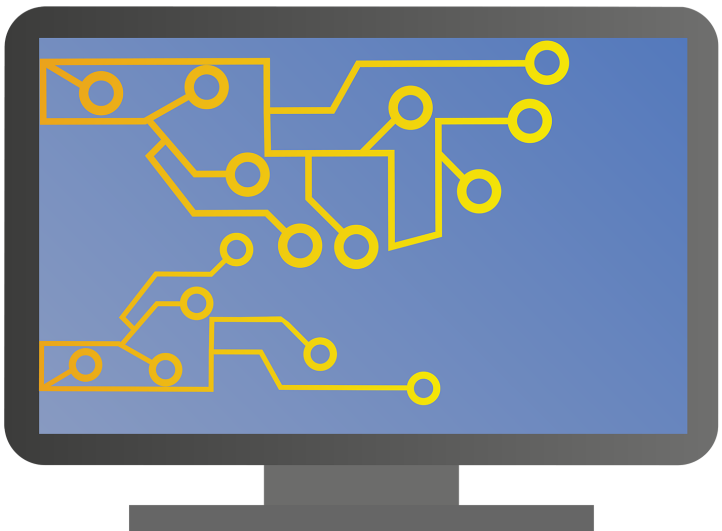
- Roll-Out-Begleitung im Unternehmen

- Outsourcing und Lieferanten-Management

- Test und Übungen

- Monitoring und Nachweislegung

Dabei ist die Größe eines Unternehmens unerheblich, da es immer angeraten ist, Vorsorge für den Ausfall zu betreiben. Zugegeben, die Komplexität steigt mit der Größe.



Rödl & Partner

VIERTENS

EIN CYBERVORFALL: ZUSTÄNDIGKEITEN, PROZESSE & INSTRUMENTE RECHTZEITIG VORHER KLÄREN

Wird ein Cyberangriff bemerkt, heißt es, schnell und sicher zu handeln. Um einen Angriff abzuwehren, heißt es, auf technischer Ebene und im Know-how gut vorbereitet zu sein. Sollte beides „ausgelagert“ werden, gilt auch hier, dass ein Dienstleister gut ausgewählt und ebenso überwacht werden muss.

In beiden Situationen (make or buy) gilt es, sich dem Thema Cybervorfall proaktiv anzunehmen und in Vorbereitung zu gehen.

Unser Leistungsportfolio umfasst dabei sowohl die Strategie, die Auswahl, die Überwachung, als auch in Teilen Unterstützender zu sein.

- Stärken-/Schwächen-Analyse in Bezug auf Cybervorfälle

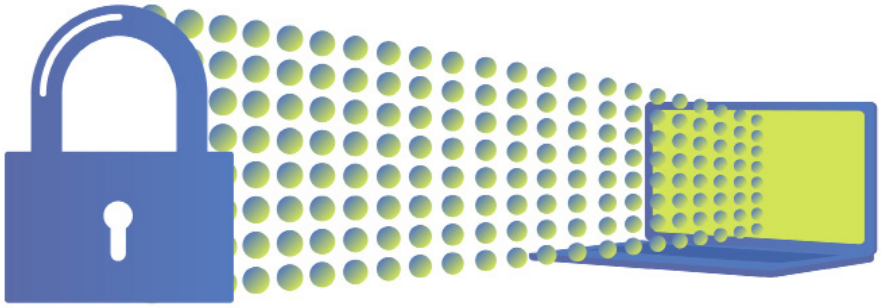
- Konzeption eines sinnvollen Cybervor fall-sammenarbeitsmodell mit verschiedenen Playern im Cybersecurity-Umfeld (laufendes Monitoring, individuelle Vorfalleinschätzung und Gegenmaßnahmen, Forensik, angezeigte Ertüchtigungsmaßnahmen, etc.)

- Ableitung von internen Unternehmensregelungen ggü. Mitarbeitenden und innerhalb der IT

- Begleitung bei der vertraglichen Gestaltung (über die Rechtsberatung der Rödl & Partner Unternehmensgruppe)

- Begleitung bei der
    - Abwehr von Angriffen
    - Zusammenarbeit mit Polizei und Behörden (Datenschutz)
    - Nachweiserstellung

Eine ähnliche Herangehensweise würde sich auch im Fraud-Fall bei Innentäter anbieten.



Kontakt

HANNES HAHN
Partner
IT-Auditor IDW, CISA, CDPSE, DSB – Datenschutzbeauftragter (TÜV), Zertifizierter CISIS12® Berater

T: +49 221 9499 092 00
M: +49 171 6323 660
hannes.hahn@roedl.com
www.roedl.de