CYBER-SECURITY SERVICES – ABWEHRFÄHIGKEIT IM CYBERSPACE.

SCHLÜSSELKOMPETENZ CYBER-ABWEHR.

Die Verwundbarkeit weltweit vernetzter Unternehmen nimmt zu. Cyber-Kriminelle, Internetaktivisten und Industriespione besitzen heute eine hohe Professionalität. Selbst Großkonzerne sind nicht mehr in der Lage, die vielfältigen Gefährdungen im Alleingang zu beherrschen. Mehr und mehr zielen die Angreifer auf die betrieblichen Kernfähigkeiten: Während Cyber-Spione an das Spitzen-Know-how wollen, mit dem sich Unternehmen im Markt differenzieren, nehmen Cyber-Saboteure genau die Geschäftsabläufe ins Visier, die für die Wertschöpfung der Unternehmen unentbehrlich sind.

Angesichts der Gefahrenzunahme wird der Aufbau einer wirksamen Cyber-Abwehr zur Schlüsselkompetenz. Corporate Governance und Corporate Risk Management sind bei dieser Aufgabe ebenso gefordert wie der IT/TK-Bereich. In der Praxis stehen Unternehmen vor der Aufgabe, vorhandene Prozesse und Mechanismen in ein unternehmensweites Cyber-Sicherheitsmanagement einzubetten. Als weltweit tätiger Ende-zu-Ende-Anbieter verfügt T-Systems über das Wissen und die Services, um in Unternehmen diesen Transformationsprozess erfolgreich zu begleiten.

UMSETZUNGSORIENTIERTE BERATUNG.

In einem grundlegenden Cyber Security Assessment analysiert T-Systems, welche Ressourcen im Unternehmen welchen Risiken ausgesetzt sind. Das Assessment zeigt den IST-Zustand der aktuellen Gefahrenabwehr und definiert das angestrebte Sicherheitsniveau. Dabei liegt der Schwerpunkt auf dem Schutz geschäftskritischer Prozesse. Darauf aufbauend entwickelt das Cyber Security Architecture Consulting eine Referenzarchitektur, aus der sich alle erforderlichen Einzelmaßnahmen konsistent ableiten lassen.

Welche Maßnahmen wie und wann umzusetzen sind, zeigt das Cyber Security Transformation Consulting. Auf Wunsch begleitet T-Systems die Umsetzung und unterstützt die Cyber-Abwehr mit erprobten Managed Services. Finden Angreifer einen Weg durch die Abwehrlinien des Unternehmens, greift der Cyber Incident Response Plan, um Wissen und Prozesse wirksam zu verteidigen.

T · · Systems ·

DIE CYBER-SECURITY SERVICES IN DER EINZELSICHT.

CYBER SECURITY ASSESSMENT.

Das Assessment klärt die individuelle Gefährdungslage des Unternehmens. Die T-Systems Security-Experten erkennen, welche Informationen, Systeme, Prozesse und Standorte wie attraktiv für welche Gruppe von Angreifern sind. Sie ermitteln das Ausmaß möglicher Schäden und analysieren die Wirksamkeit der gegenwärtigen Gefahrenabwehr. Dabei übernehmen die Experten die Rolle von Angreifern und versuchen u.a. mit so genannten Penetrationstests die Schutzsysteme zu überwinden. Sind die Cyber-Risiken identifiziert und bewertet, definieren die Berater von T-Systems zusammen mit dem Kunden das erforderliche Sicherheitsniveau. Im Ergebnis liefert das Assessment ein aussagekräftiges SOLL/IST-Modell, aus dem sich geeignete Maßnahmen ableiten und priorisieren lassen.

CYBER SECURITY ARCHITECTURE CONSULTING.

Vor dem Hintergrund der Assessment-Ergebnisse entwickelt T-Systems eine Cyber-Referenzarchitektur. Die bestehende IT/TK-Infrastruktur dient dabei als Ausgangspunkt, um die bisherigen Investitionen so weit wie möglich zu schützen. Falls das bestehende Sicherheitsmanagement die identifizierten Risiken nicht ausreichend abdeckt, zeigt die Referenzarchitektur präzise auf, an welchen Stellen eine Transformation erforderlich ist.

CYBER SECURITY TRANSFORMATION CONSULTING.

Ergibt der SOLL/IST-Abgleich einen Handlungsbedarf, setzt T-Systems eine Roadmap mit konkreten Maßnahmen auf und priorisiert die Aufgaben. Für jede Maßnahme ist ablesbar, welchen Beitrag sie zur Abwehrfähigkeit des Unternehmens leistet. Um den angestrebten Nutzenzuwachs überprüfbar zu machen, definieren die T-Systems Berater individuelle Kennzahlen und stellen Messmethoden bereit.

CYBER INCIDENT RESPONSE.

Zudem entwickelt T-Systems ein systematisches Vorgehen für das Management von Sicherheitsvorfällen. Es bildet das Rückgrat der operativen Angriffsabwehr und unterstützt weiterführende Aufgaben wie Informationspolitik oder Beweissicherung. Neben eigenen Erfahrungswerten orientiert sich T-Systems dabei u.a. an Industriestandards wie ISO/IEC 27035 oder den NIST Special Publications 800-61 und 800-86.

CYBER INTELLIGENCE FÜR DIE IT/TK-INFRASTRUKTUR.

Zusätzlich zu den Beratungsleistungen bietet T-Systems einen Cyber-Intelligence Service, der rund um die Uhr arbeitet. Dieser Service greift auf Informationen aus verschiedenen Informationsquellen zu und bewertet sie. Als Informationsquelle dient dabei zum Beispiel ein Security Information & Event Management (SIEM), das T-Systems als Managed Service betreibt. Es fasst die Log-Daten aller sicherheitsrelevanten Systeme zusammen und wertet sie permanent aus. Im Angriffsfall übernimmt ein Cyber Incident Response Team von T-Systems die Kontrolle und wehrt die Attacke ab.

DIE CYBER-SECURITY SERVICES.

- machen Risiken und Cyber-Schutz kalkulierbar und bieten eine Roadmap zu optimaler Abwehrfähigkeit
- verbessern die Reaktionsfähigkeit und begrenzen die Schadenshöhe im Falle eines Angriffs
- halten die Verfügbarkeit von Informationen, Systemen und Prozessen und damit den laufenden Betrieb aufrecht
- sichern den Entwicklungsvorsprung gegen Spionage
- begrenzen Kosten durch Vertragsstrafen oder Sanktionen und vermeiden Imageschäden
- schaffen eine gemeinsame Arbeitsbasis für Corporate Governance, Risk Management und IT/TK-Bereich

HABEN SIE NOCH FRAGEN?
Internet: www.t-systems.de/security
oder schreiben Sie eine E-Mail an
security-info@t-systems.com

EXPERTENKONTAKT
T-Systems International GmbH
Gerd Enste
Vorgebirgsstr. 49
53119 Bonn

HERAUSGEBER
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt
Deutschland

Stand 02/2013 | Änderungen und Irrtümer vorbehalten