PRÄVENTION. DETEKTION. REAKTION.

Beratung, Services und Technologien für eine ganzheitliche Cyber Defence

Längst ist klar, dass sich Unternehmen nicht mehr nur mit präventiven Maßnahmen vor Cyberkriminellen schützen können. Detektion und Reaktion sind mittlerweile im Rahmen einer Cyber-Defence-Strategie unabdingbar. Statt Best-of-Breed sollte der Best-Integrated-Ansatz im Vordergrund stehen: Lösungen, die sich bestmöglich miteinander verzahnen lassen, um eine ganzheitliche Sicht auf die Security zu ermöglichen.

EINEN 100-PROZENTIGEN SCHUTZ GIBT ES NICHT …

Jedes Unternehmen muss sich vor Cyber-Angriffen schützen. Hacker – ob Kriminelle, Geheimdienste oder Wettbewerber – entwickeln mit viel Kreativität und Können ständig neue Angriffsvarianten. Um diesem Trend zu begegnen, wird der Markt von neuen Anbietern und Produkten geflutet, die alle bestmöglichen Schutz versprechen. In Summe ist deshalb nicht nur die IT-Sicherheit selbst, sondern auch der Markt für IT-Sicherheitslösungen sehr komplex und unübersichtlich geworden. Beide Entwicklungen machen es Unternehmen nicht unbedingt leichter, ihre Security-Strategie in Technologie umzusetzen.

… ABER WERKZEUGE ZUR ABWEHR VON ANGRIFFEN

Die beste IT-Sicherheitslösung ist daher diejenige, die sich aus einer ausgewogenen Mischung aus Prävention, Detektion und Reaktion zusammensetzt und die gesamte IT-Infrastruktur umfasst: vom Netzwerk über die Server und Services bis hin zu den Endgeräten. Um diese verschiedenen Aspekte zu einer integrierten Lösung zu vereinen, müssen sich die einzelnen Teile wie ein 3D-Puzzle zusammenfügen und technologisch integrieren lassen. Denn mit integrierten Werkzeugen zur Konsolidierung sowie Automatisierung lassen sich im Verdachtsfall Analysen deutlich schneller und effizienter durchführen.

Dabei spielt die technologische Integration eine ganz entscheidende Rolle. Diese umfasst Werkzeuge und Technologien wie

- User und Entity Behaviour Analytics (UEBA)
- Security Information and Event Management (SIEM)
- Security Incident Response Plattformen (SIRP)
- Forensik und Incident Response
- Threat Intelligence Feeds

UNSER VERSPRECHEN: EINE PASSGENAUE CYBER DEFENCE

Als langjährig erfahrener IT-Dienstleister kennt Computacenter die Bedürfnisse von Unternehmen und Behörden sehr genau.

Gemeinsam mit unseren Kunden entwickeln wir individuelle Cyber Defence-Strategien, wählen die Lösungen aus, die am besten zur bestehenden Infrastruktur passen und implementieren diese.

Um schnell und effizient auf Angriffe reagieren zu können, unterstützen wir unsere Kunden außerdem beim Auf- und Ausbau von Security Operations Centern (SOC) oder Cyber Defence Centern (CDC). Weil ein gut funktionierendes SOC oder CDC sich ständig weiterentwickeln muss, Fachkräfte aber rar sind, helfen wir mit Security-Analysten und Krisenmanagern on-demand immer dann aus, wenn Spezialisten gebraucht werden.

CYBER DEFENCE PORTFOLIO

CONSULTING

- SOC/CDC Aufbau
  - Lagebilderstellung inkl. KPIs
  - Prozesse, Rollen & Organisation
  - Technologien
- SOC Weiterentwicklung/ Optimierung
  - SOC Maturity Assessment und Benchmarking
  - SOC Optimierung
- Transition & Change
  - SOC Service Provider Selektion (Tier 0 – Tier 4)
  - SOC Sourcing Beratung (in/out/re-sourcing)

SERVICES

- Ereignis- und Vorfallsanalysen
- Vorfallsbehandlung
- Krisenmanagement
- Schadcode-/Malware-Analysen
- Threat Intelligence/ Darknet-Analysen
- Hunting on Demand
- Pentesting von Infrastrukturen (Ethical Hacking Red-Team-Testing)

→ durchgeführt von Krisenmanagern und/oder Security Analysten

TECHNOLOGIEN

- Security Information & Event Management (SIEM)-Lösungen
- Tools für User und Entity Behaviour Analytics (UEBA)
- Security Incident Response Platformen (SIRP)
  - Case-Management-Lösungen
- Forensik & Incident Response Tools
- Threat Intelligence Feeds/ Informationen

INFORMATIONSQUELLEN FÜR DAS SOC UND ORCHESTRIERTE SICHERHEITSLÖSUNGEN IN DER KUNDENINFRASTRUKTUR
Infrastructure Security, Network-Security, Endpoint-Security-Lösungen, Identity & Access Management, Advanced Malware Protection (AMP), Vulnerability Management, Cloud Security, Risiko Management, Content Management Database (CMDB).

DIGITAL & Trust. Mastering business security

Computacenter

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

computacenter.de
+49 (0)2273 5970