PRÄVENTION. DETEKTION. REAKTION.

Best-Integrated-Konzepte für ganzheitliche Cyber Defence

Längst ist klar, dass sich Unternehmen nicht mehr nur mit präventiven Maßnahmen vor Cyberkriminellen schützen können. Heutzutage sind Detektion und Reaktion im Rahmen einer Cyber-Defence-Strategie unabdingbar. Während der Fokus bislang auf dem Best-of-Breed-Gedanken lag – also die besten Lösungen mit den meisten Features zu implementieren –, sollte künftig 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.

Insbesondere weil es sich bei der Analyse von Sicherheitsvorfällen häufig um die sprichwörtliche Suche nach der Nadel im Heuhaufen handelt, sollten Big-Data-Technologien zum Einsatz kommen, um die enormen Datenmengen überhaupt bewältigen zu können – aus klassischen SIEM-Lösungen wird damit SIEM 2.0, der nächste logische und notwendige Schritt bei der Cyber Security. Folglich spielt die technologische Integration eine ganz entscheidende Rolle. Diese umfasst Werkzeuge und Technologien wie

- Advanced Analytics wie User Behaviour Analytics (UBA)
- Security Information and Event Management (SIEM)
- klassische Netzwerk-Security-Lösungen
- Advanced-Endpoint-Security-Lösungen
- Advanced Malware Protection (AMP)
- Security Incident Management Tools
- sowie Security Intelligence Feeds.

INTEGRATIONSGEDANKE IST TEIL UNSERER DNA

Als langjährig erfahrener IT-Dienstleister kennt Computacenter die Bedürfnisse von Unternehmen und Behörden sehr genau. Im Rahmen einer Cyber-Defence-Strategie entwickeln wir gemeinsam mit unseren Kunden individuelle IT-Sicherheitskonzepte und integrieren die erforderlichen technologischen Komponenten.

Immer am Puls der Zeit, analysieren wir kontinuierlich neue IT-Sicherheitslösungen am Markt – sowohl von bewährten Herstellern als auch von Startup-Unternehmen – und passen unser Portfolio stetig neu an.

Im Vordergrund stehen dabei die Integrationsmöglichkeiten der einzelnen Lösungen in ein ganzheitliches Konzept. Dadurch sind wir in der Lage, unseren Kunden die für sie beste Lösung anzubieten. Immer unter dem Aspekt des Best-Integrated-Ansatzes.

Computacenter

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

computacenter.de
+49 (0)2273 5970