Cybersecurity 360°: planen – bauen – betreiben
Bedrohungen aufdecken – Verteidigung verbessern

Für den Erfolg Ihres Kerngeschäfts ist das reibungslose Funktionieren Ihres Netzwerks mit all seinen IT-Dienstleistungen unerlässlich. Systemausfälle durch Hackerangriffe oder der Verlust sensibler Daten schaden dem Image und führen schnell zu finanziellen Einbussen. Damit Ihnen dies nicht passiert, unterstützt Sie die Cybersecurity-Spezialistin terreActive bei der Planung und dem Aufbau Ihrer Cyber-Defense-Lösung sowie auf Wunsch auch beim Betrieb Ihrer IT-Sicherheitsinfrastruktur rund um die Uhr.

Standortbestimmung und Planung

Können Sie mit Bestimmtheit sagen, dass Sie noch nie angegriffen wurden und sich der Hacker nicht schon längst unentdeckt in Ihrem Netzwerk bewegt? Mittels Security-Assessment können Sie Ihr Risiko besser einschätzen und Ihre bestehenden Massnahmen überprüfen lassen. Basierend auf den Ergebnissen erarbeitet terreActive gemeinsam mit Ihnen ein langfristiges Konzept und schlägt Ihnen eine Defense-Strategie inklusive der passenden Plattform vor. Für einen optimalen Investitionsschutz werden bereits installierte Tools genutzt und neue schrittweise integriert, um die Cyber Defense stetig zu erhöhen und den wachsenden Anforderungen gerecht zu werden.

Concepts
Assessments
Architectures
Cyber Deception
Risk & Compliance

Audits
Penetration Tests
Vulnerability Scan
Social Engineering
Phishing Simulation
Awareness Trainings

SOC Services
Forensic Analysis
Incident Response
SOAR-as-a-Service
Operations Control
Security Monitoring
Vulnerability Management
Managed Security Services
System Monitoring & Maintenance
Threat Detection & Intelligence & Hunting

WAF
SIEM
Firewall
Network Security
Log Management
Application Security
Web & E-Mail Security
Cyber Defense Platform
Privileged Access Control

Cyber Defense Center

Hacker schlafen bekanntlich nicht und Security-Ressourcen sind in vielen Unternehmen knapp. Damit Sie sich trotzdem auf Ihr Kerngeschäft konzentrieren können, kümmert sich terreActive um den Betrieb (Operations) Ihrer Sicherheitsinfrastruktur. Sie können nach Bedarf nur einzelne Services oder ein 7x24-Komplettpaket buchen. Die Security Engineers und Analysts aus der Schweiz unterstützen flexibel auch Ihr eigenes SOC (Security Operations Center) mit Managed Services.

Ihre Vorteile

– Assessment und Standortbestimmung Ihrer aktuellen Cyber Security
– Ergänzung Ihrer Organisation und Entlastung Ihrer internen Security-Ressourcen durch gezielte Services
– 7x24-Überwachung Ihrer IT-Sicherheitsinfrastruktur
– Lokal und verfügbar: 365 Tage Full-Time-Service durch ausgewiesene Security-Expertinnen und -Experten in der Schweiz
– Bedrohungen frühzeitig erkennen und Schwachstellen beheben
– Alarmierung bei Sicherheitsvorfällen sowie schnelle Reaktion
– Modularer Servicekatalog mit flexiblen Laufzeiten bei voller Kostenkontrolle
– Durch die langjährige Projekterfahrung zielen die Konzepte auf eine einfache Integration und einen effizienten Betrieb ab
– Mehr als 25 Jahre Security-Expertise
– terreActive ist ISO 27001 zertifiziert

Effizientes Vorgehen: die 7-Steps-Methodik

Der Security Monitoring Cycle von terreActive hilft Ihnen, Security Monitoring erfolgreich einzuführen und kontinuierlich zu verbessern. Mit der 7-Steps-Methode kommen Sie schnell zu Resultaten und können Ihr Unternehmen effizient vor Angriffen schützen. Der Security Monitoring Cycle kann auf einzelne Bereiche, z. B. auf spezifische Applikationen, oder auf ganze IT-Infrastrukturen angewendet werden. terreActive hilft Ihnen, den Fokus auf die richtigen Komponenten zu legen.

1. Review
GAP-Analyse Ihrer aktuellen Situation, Definition der notwendigen Schritte, um Ihre Ziele zu erreichen. Haben Sie bereits eine Lösung im Einsatz, geht es darum, die Effektivität des Security Monitorings zu überprüfen und kontinuierlich zu verbessern.

2. Concept
Auf Basis des vorgängig durchgeführten Reviews werden die konzeptionellen Aspekte der Lösung erarbeitet. Dies reicht von der richtigen Dimensionierung und Architektur der Lösung über die Vorgaben-konforme Integration der Log-Quellen bis zur Stakeholder-angepassten Auswertung. Dadurch werden klare Vorgaben für die spätere Umsetzung definiert, die eine gute Projektkontrolle ermöglichen, und eventuelle Vorbehalte werden vor weiteren Investitionen sichtbar.

3. Collect
Hier erfolgt der Aufbau des Security Monitoring Frameworks und die Anbindung und Parametrisierung der Log-Quellen gemäss Konzept. Ein wichtiger Punkt in dieser Phase ist die Inventarisierung und Klassifizierung der anfallenden Log-Daten.

4. Analyse
Nach der zentralen Sammlung aller relevanten Log-Daten führt die Anreicherung und Aufbereitung der Daten mittels Analyse-Tools zu verbesserter Transparenz und erhöht damit die IT-Sicherheit enorm.

5. Detect
Ziel ist es, möglichst hoch automatisiert anhand von gesammelten Daten sicherheitsrelevante Ereignisse zu detektieren. Dies kann beispielsweise das Versiegen einer Log-Quelle oder eine Brute-Force-Attacke auf einen Benutzer-Account sein. Die Detektion von gezielten Angriffen (z. B. APT Advanced Persistent Threat) oder unzufriedenen Administratoren, die sensitive Daten abziehen, sind oft nur per Know-how von ausgewiesenen Security Engineers möglich.

6. React
Die Alarmierung wird über eingespielte Prozesse an die Expertinnen und Experten, die meist in einem Security Operations Center (SOC) organisiert sind, weitergeleitet. Diese bestimmen die Gefährlichkeit und Dringlichkeit des Vorfalls und leiten die notwendigen Massnahmen ein. Die Effektivität dieser Phase hängt stark von den Ressourcen, der Reaktionszeit und dem Expertenwissen ab. Idealerweise müssten daher eine 7x24-Organisation und Ressourcen mit dem notwendigen Know-how bereitgestellt werden.

7. Report
Reporting ist ein integraler Bestandteil des Security Monitorings und dient zur Transparenzsteigerung und Beweisführung. In regelmässigen Meetings mit den Security Analysts werden die Reports besprochen und Schwachpunkte analysiert.

Cloud oder On-Premises, auf jeden Fall sicher

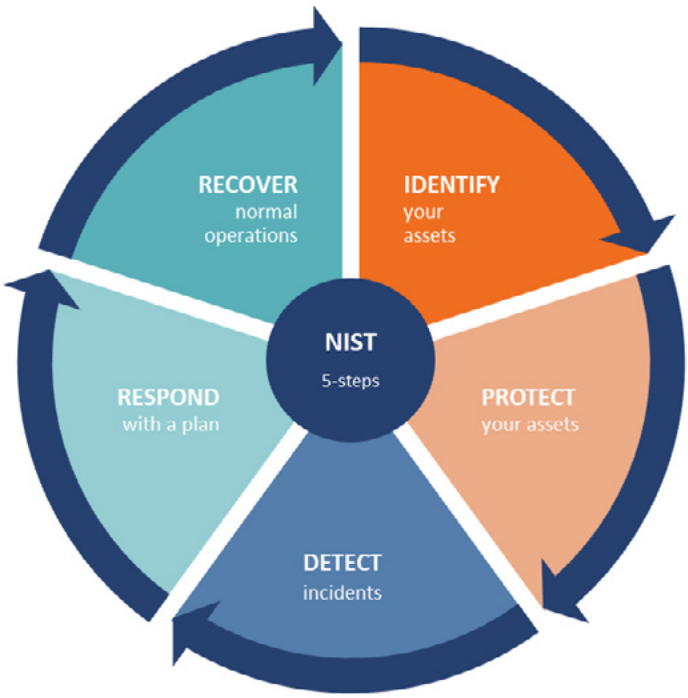
Viele Organisationen verlegen ihre IT heutzutage in die Cloud. Aber Achtung: Nicht alle Verantwortungen können an den Cloud-Provider ausgelagert werden. Gemeinsam mit Ihnen prüft terreActive, für welche Bereiche Sie die Security sicherstellen müssen, und empfiehlt Ihnen geeignete Massnahmen. Die operative Überwachung übernehmen, egal ob in der Cloud oder On-Premises, die Security Engineers und Analysts von terreActive im eigenen SOC in Aarau.

Sicherheit durch Schweizer und internationale Standards

Ausgerichtet auf die Bedürfnisse Ihrer Organisation und Ihrer Ziele empfiehlt terreActive Ihnen, an welchem Standard Sie sich orientieren sollten. Hier nur zwei mögliche Beispiele.

IKT-Minimalstandard
Der IKT-Minimalstandard wurde vom Bundesamt für wirtschaftliche Landesversorgung BWL lanciert und bietet allen Organisationen eine Hilfestellung zur Stärkung der eigenen Cybersicherheit. Er enthält Empfehlungen und Orientierungspunkte für eine bessere Widerstandsfähigkeit gegen Cyberangriffe. Ein Security-Audit nach dem IKT-Minimalstandard bietet Ihnen einen guten Einstieg in Ihre Planung.

NIST
NIST, das National Institute of Standards and Technology, stellt ein Cyber Security Framework zur Verfügung, an dem sich Ihre Verteidigung orientieren sollte. Für jede der fünf Phasen benötigen die Security Engineers geeignete Tools und Services, die als Ganzes die Cyber-Defense-Plattform Ihrer Organisation bilden. terreActive berät Sie gerne dabei, welche für Sie sinnvoll sind. terreActive empfiehlt, klein zu starten und nach und nach auszubauen, um die Security-Maturität stetig zu verbessern.



Zusätzlich zu den allgemeinen Security-Standards gilt es in vielen Branchen Besonderheiten zu berücksichtigen wie beispielsweise die Anwendung der FINMA-Regeln im Bankensektor. Ob Healthcare, Government oder Industry (OT), die Security Consultants von terreActive unterstützen Sie fallbezogen mit auf Sie zugeschnittenen Use Cases.

Post CH Kommunikation AG
E-Government
Wankdorfallee 4
3030 Bern
Schweiz

E-Mail egovernment@post.ch
post.ch/e-government