Netzwerkbezogener Sicherheitsansatz:

Network Detection & Response (NDR) als Teil der Cyber Defense Strategie

IT Security Teams stehen in Anbetracht der zahlreichen und fortschrittlichen Cyberbedrohungen vor der Herausforderung, für Unternehmen eine aktive, schnelle und umfassende Cyber Detection & Response sicherzustellen. Um dieses Ziel zu erreichen, kommen unterschiedlichste „Threat Detection and Response" Tools in Frage, die das Ziel haben, stattfindende Angriffsaktivitäten zeitnah aufzuspüren, zu melden und somit die Cyber Resilience umfassend und nachhaltig zu erhöhen. Network Detection & Response (NDR) spielt hierbei eine maßgebliche Rolle und sollte – ergänzt um weitere Services – einen festen Platz in der Cyber Defense Strategie von Unternehmen einnehmen.

Mit dem netzwerkbezogenen Sicherheitsansatz Network Detection and Response (NDR) kann der gesamte Datenverkehr eines Unternehmens kontinuierlich überwacht und analysiert werden - basierend auf statischen Regeln, Machine Learning und Threat Intelligence. Die Lösung bezieht dabei sowohl den gesamten internen Datenverkehr als auch die externe Kommunikation ein, berücksichtigt also Quellen wie beispielsweise Client- und Serversysteme, Netzwerkkomponenten, aber auch IoT-Sensoren oder OT-Geräte. Das somit erreichte tiefgehende Verständnis des normalen Netzwerkverhaltens führt zu einer zuverlässigen und schnellen Identifizierung von Anomalien.

Die 6 wichtigsten Merkmale von NDR sind:

- Überwachung von Netzwerkverkehr: Eine NDR-Lösung überwacht und analysiert den Netzwerkverkehr hinsichtlich potenzieller Bedrohungen. Dies kann durch die Verwendung von Technologien wie Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS) erfolgen.
- Verhaltensanalyse: Eine NDR-Lösung verwendet Machine Learning-Algorithmen, um das verhaltensmäßige Muster des Netzwerkverkehrs zu analysieren und Anomalien zu erkennen, die auf eine mögliche Bedrohung hinweisen können.
- Automatische Reaktion: Eine NDR-Lösung kann automatisch auf erkannte Bedrohungen reagieren, indem sie z.B. Netzwerkverbindungen trennt oder Regeln im Firewall-System implementiert.

- Integritätsschutz: Eine NDR-Lösung kann auch dafür sorgen, dass die Integrität des Netzwerks durch Überwachung von Änderungen an Konfigurationen und durch Überwachung von unbefugten Zugriffen auf Netzwerkressourcen gewahrt wird.
- Berichterstattung und Forensik: Eine NDR-Lösung bietet die Möglichkeit, detaillierte Berichte und Forensik-Daten zu erstellen, die bei der Untersuchung von Sicherheitsvorfällen und bei der Identifizierung von Angreifern hilfreich sind.

Um jedoch eine effektive, nachhaltige und zuverlässige Bedrohungserkennung realisieren zu können, bedarf es des Zusammenspiels von NDR mit weiteren Lösungen.

Netzwerkbedrohungen erkennen und gezielt darauf reagieren

Durch die systematische, automatisierte Überwachung des Datenverkehrs und des Netzwerkverhaltens lernen NDR-Lösungen das „normale Verhalten“. Treten von diesem gelernten Verhalten abweichende Muster auf, wie beispielsweise verdächtige Zugriffe auf Systeme oder Datenexfiltrationen, wird durch die NDR-Lösung automatisiert ein Alarm ausgelöst.

Idealerweise sollten die Alarme zentral gesammelt werden, beispielsweise in einem **SIEM-System** (Security Information and Event Management) und mit weiteren Daten, beispielsweise von einer **EDR-Lösung** (Endpoint Detection and Response), korreliert werden. Mithilfe des SIEM kann der Cyber Defense Analyst auftretende Unregelmäßigkeiten zentral und effizient analysieren und falls nötig gezielt darauf reagieren. Von Vorteil ist hierbei die Unterstützung durch ein **SOAR-System** (Security Orchestration Automation and Response).

Die Folge des Zusammenspiels dieser Detection & Response Lösungen ist ein deutlich verbessertes IT-Sicherheitsniveau für Unternehmen, durch das erreicht werden kann, dass selbst hochentwickelte Cyberangriffe so frühzeitig identifiziert und abgewehrt werden können.

So kann NDR das SIEM unterstützen

Sowohl NDR als auch SIEM sammeln und teilen Informationen und arbeiten auf dieser Basis mit dem übergreifenden Ziel zusammen, Bedrohungen zu erkennen, zu verifizieren und darauf zu reagieren.

Nach der Identifizierung eines Angriffs kann eine NDR-Lösung automatisch reagieren, indem es die betroffenen Geräte isoliert, um die Ausbreitung des Angriffs zu verhindern und die betroffenen Bereiche zu bereinigen. Des Weiteren stellt die NDR-Lösung alle gesammelten Informationen dem SIEM-System zur Verfügung.

Im Einzelnen unterstützt NDR das SIEM durch:

- Erfassung und Analyse von Verbindungsdaten aus dem Netzwerkverkehr

- Bereitstellung einer unveränderlichen Datenquelle
- Optimierung von vollständigen, umfassenden Berichten
- Abdeckung von Protokolllücken
- Protokollanalysen sowie Aggregation und Erkennen verhaltensbedingter Bedrohungen

Das SIEM nutzt diese Informationen zusammen mit weiteren Ereignissen von verschiedenen Sicherheitsgeräten und -anwendungen in Echtzeit und korreliert diese Daten, um potenzielle Bedrohungen zu erkennen und Alarme zu generieren. Auch Cyber Defense Analysten verwenden die Informationen, die durch NDR gesammelt werden, um wiederum die Erkennungsregeln im SIEM anzupassen und zukünftige Angriffe besser zu erkennen und abzuwehren.

Die Ergänzung von NDR mit EDR

Der Fokus von Endpoint Detection & Response (EDR)-Lösungen liegt auf der Erhöhung der Visibilität von Anomalien auf dem Endpunkt: Der Schutz findet direkt auf den Endgeräten und nicht an der Netzwerkgrenze statt. Endpunkte – also alle Geräte, die mit einem Netzwerk verbunden sind – stellen potenzielle Einfallstore für Cyberbedrohungen dar. Mit **EDR** werden die Aktivitäten der Endgeräte in Echtzeit erfasst, protokolliert und analysiert. Somit stellen EDR-Lösungen einen wertvollen Bestandteil des Cyber Defense-Toolsets dar, sind jedoch durch ihren Fokus auf Endgeräte nicht in der Lage, Netzwerkverkehr und -aktivitäten zu überwachen, die außerhalb des Endgeräts stattfinden. Diese Art von Überwachung und Analyse erfordert eine Network Detection and Response (NDR)-Lösung. Die Technologien ergänzen sich somit ideal und führen dazu, dass durch die Korrelation der gewonnenen Informationen ein detaillierteres Sicherheitsbild entsteht und Angriffe umfassend erkannt und abgewehrt werden können.

Fazit

Nach wie vor vertrauen SOC-Teams bei ihrer Arbeit in hohem Maße auf Tools zur Erkennung und Reaktion von Endpunkten (EDR) sowie zur Verwaltung von Sicherheitsinformationen und Ereignissen (SIEM). Diese Tools können jedoch keinen Einblick in den Datenverkehr bieten und geben somit nur einen kleinen, sehr begrenzten Ausschnitt über sicherheitsrelevante Vorgänge. Erst durch die Ergänzung mit einem NDR können Cyberangriffe frühzeitig erkannt, analysiert und gezielt abgewehrt werden. Die Kombination von NDR, EDR und SIEM ermöglicht es, Bedrohungen und Angriffe auf Anwendungs-, Netzwerk- und Endpunktebene zu erkennen und umgehend zu reagieren.

Autoren: Ramon Weil - Founder & CEO - SECUINFRA GmbH

Norbert Nitsche - Head of Cyber Detection & Response Center - SECUINFRA GmbH

Weitere Informationen: https://www.secuinfra.com/de/techtalk/die-rolle-von-network-detection-response-bei-der-effektiven-bedrohungserkennung/

Kontakt: SECUINFRA GmbH

Svenja Koch

Stefan-Heym-Platz 1

10367 Berlin

Deutschland

Tel. +49 (0) 160 921 633 44

svenja.koch@secuinfra.com