Schützen Sie Ihr Unternehmen mit Endpoint Detection and Response (EDR)

EDR – eine Hauptwaffe in Ihrem Cybersicherheitsarsenal

Ransomware und Datendiebstahl können Ihre Geschäftsabläufe lahmlegen, wertvolle Daten gefährden und Ihren Ruf schädigen. Um Ihr Unternehmen zu schützen, benötigen Sie eine robuste, mehrschichtige Sicherheitslösung, die eingehende Gefahren erkennt und in Echtzeit auf Cyberbedrohungen reagiert.

Endpoint Detection and Response (EDR) ist ein wesentlicher Bestandteil der heutigen zuverlässigen Cyberabwehrstrategien. Es kombiniert die Fähigkeiten zur Erkennung von Bedrohungen durch modernste KI-Algorithmen und maschinelles Lernen mit der Fähigkeit, eingehende Bedrohungen angemessen und entschlossen zu bekämpfen.

EDR schützt diese wichtigen Unternehmensressourcen:

· Desktops

· Laptops

· Tablets

· Server

· Smartphones

· IoT-Geräte (Internet of Things)

Herkömmliche Antivirus-Lösungen reichen nicht mehr aus, um die sich weiterentwickelnden Taktiken von Cyberkriminellen zu bekämpfen. Warum? Weil Antivirus-Software auf Datenbanken basiert, die der Erstellung und dem Einsatz von Angriffen durch Cyberkriminelle hinterherhinken. Von der Bekämpfung von Kriminellen, die ausgefeilte Ransomware gegen Ihr Unternehmen einsetzen, bis hin zur Abwehr von Zero-Day-Exploits – EDR erkennt und bekämpft die Bedrohungen, die Ihren Daten, Prozessen und Ihrem Ruf schaden könnten.

Die Vorteile von EDR

· **Identifizierung von Zero-Day-Bedrohunge** – Unterstützung bei der Verteidigung Ihres Unternehmens gegen die Flut neuer und aufkommender Angriffe von Cyberkriminellen

· **Echtzeitreaktion** - hilft Ihnen, Bedrohungen einzudämmen und zu entschärfen, bevor sie erheblichen Schaden anrichten.

· **Umfassende Sichtbarkeit** – sorgt für Transparenz in Ihrem gesamten Netzwerk und bietet detaillierte Einblicke in Art und Umfang der Bedrohungen.

· **Datengestützte Analyse** - bietet umsetzbare Informationen zur Verbesserung Ihrer Sicherheitslage. Erkennen Sie Muster, sagen Sie potenzielle Bedrohungen voraus und passen Sie Ihre Abwehrmaßnahmen entsprechend an.

Hauptmerkmale unserer EDR-Lösung

- **Integration von Bedrohungsdaten**
- **Automatisierte Reaktion auf Vorfälle**
- **Verhaltensanalyse**
- **Skalierbarkeit und Flexibilitä**



Gemeinsam noch leistungsfähiger – EDR als Teil Ihres Cybersicherheitsarsenals

EDR (Endpoint Detection and Response) ist zwar ein Eckpfeiler jeder robusten Cybersicherheitsstrategie, aber nur ein Teil eines umfassenden Abwehrmechanismus, der zum Schutz eines Unternehmens erforderlich ist.

Für ein umfassendes Schutzarsenal müssen Unternehmen wie Ihres eine Datenverschlüsselung einführen, um sensible Informationen zu schützen, sowie BCDR-Pläne (Business Continuity and Disaster Recovery), damit Sie bei Störungen auf einem gewissen Niveau weiterarbeiten können.

Aber das ist noch nicht alles.

DNS-Filterung ist erforderlich, um den Zugriff von Mitarbeitern auf schädliche Websites zu verhindern, E-Mail-Sicherheit schützt vor Phishing-Angriffen und MDR (Managed Detection and Response) bietet Live-Expertenüberwachung und schnelle Reaktion auf Vorfälle.

Diese Protokolle und Tools schaffen, wenn sie in EDR integriert sind, eine mehrschichtige Sicherheitsumgebung, die Ihr Unternehmen vor eingehenden Cyber-Bedrohungen schützt.

Benötigen Sie weitere Informationen?

ThornTech-IT
thorntech-it.de
info@thorntech-it.de
015901437360

About Us