Zukunftssichere Endpoint Security

Der umfassende Schutz von Endgeräten fordert die IT-Security heraus – dies namentlich angesichts der zunehmenden mobilen Arbeit ausserhalb der IT-Firmeninfrastruktur sowie raffinierter werdender Bedrohungen. Konventionelle Sicherheitslösungen genügen nicht mehr. Zeit, einen Blick auf «Endpoint Detection and Response» (EDR) zu werfen.

Einfache Malware – zum Beispiel Viren, Trojaner und Spyware – bildet mit rund 90 Prozent nach wie vor den Hauptanteil der Cyberbedrohungen. Doch die restlichen 10 Prozent haben es in sich: Die Folgen von Advanced Persistent Threats (ATP), von dateilosen, komplexen und zielgerichteten Angriffen, verursachen pro Vorfall massiv höhere Kosten als ein simpler Virenbefall.

Klassische Endpoint-Protection-Lösungen können solche fortgeschrittenen Attacken nicht abwehren – und in der Regel auch nicht erkennen. Hinzu kommt, dass firmeninterne IT-Security-Teams (sofern überhaupt vorhanden) chronisch überlastet sind und oft nicht über die Ressourcen und das Know-how verfügen, um einen wirksamen Endgeräteschutz zu gewährleisten. Laut der Kaspersky Global Corporate IT Security Risks Survey sind sich rund 40 Prozent der KMUs nicht bewusst, welchen Bedrohungen sie wirklich ausgesetzt sind.

Malware-Attacke ohne Dateien

Ein wesentliches Problem ist dateilose Malware, die sich Mitarbeitende auf präparierten Websites oder über bösartige E-Mails einfangen. Dabei wird auf das Endgerät selbst keine Malware geschleust und der Angriff hinterlässt keine Spuren. Nichtsdestotrotz ist der Schadcode in der Lage, das betroffene System auszuspionieren, Daten abzugreifen und andere Schädlinge nachzuladen. Besonders tückisch sind dateilose Bedrohungen, die verschlüsselte Daten in der Registry ablegen, sodass sie beim Neustart automatisch geladen werden. Solche Angriffe sind für die meisten Intrusion-Prevention- und Antivirus-Lösungen praktisch unsichtbar und zehnmal häufiger erfolgreich als dateibasierte Attacken.

Nicht minder gefährlich sind gezielte Attacken – etwa per Social Engineering oder durch vorgängige Untersuchung der vorhandenen Endpoint-Security-Mechanismen und Ausnutzen von Schwachstellen. Eine weitere Variante sind Advanced Persistent Threats. Dabei nutzen Cyberkriminelle diverse Methoden, um den Angriff möglichst lange und breitflächig auf das ganze Netzwerk auszudehnen und das Unternehmen so dauerhaft zu kompromittieren.

EDR – wichtig im Kampf gegen Cyberangriffe

Ein neues Konzept, um all die raffinierten Angriffsmethoden aufzudecken und abzuwehren, nennt sich Endpoint Detection and Response, kurz EDR. Mit einer EDR-Lösung lassen sich durch Echtzeitüberwachung und zentrale Visualisierung aller Endpunkte komplexe Bedrohungen rasch erkennen, analysieren und geeignete Abwehrmassnahmen ergreifen. Die Basis dazu bilden Technologien wie eine Detection Engine mit Strukturanalysefunktion, kontinuierliche Speicherüberwachung mit Suche nach auffälligen Verhaltensmustern, Threat Intelligence aus verschiedenen Quellen und Forensik-Tools zur Vorfalluntersuchung.

Gleichzeitig arbeiten EDR-Lösungen mit automatisierten Prozessen und entlasten dadurch das IT-Team. So erreichen Unternehmen ein höheres Mass an Sicherheit, ohne dafür mehr Geld, Zeit und Know-how aufwenden zu müssen. EDR liefert Kontextinformationen zu individuellen Endpoint-Ereignissen und korreliert einzelne Ergebnisse zu Vorfällen, um Taktiken, Aktivitäten und Methoden der Bedrohung zu verstehen.

EDR funktioniert jedoch nicht im luftleeren Raum. Eine EDR-Lösung ergibt nur dann Sinn, wenn bereits ein solides Fundament an Endpoint Security vorliegt. Zur durchgängigen Bekämpfung von Cyberbedrohungen empfiehlt sich ein mehrschichtiger Ansatz: Eine klassische Endpoint-Protection-Plattform (EPP) wie Kaspersky Endpoint Security for Business macht der Mehrzahl der Malware den Garaus. Die EDR-Plattform, bei Kaspersky EDR Optimum genannt, kann sich danach auf den gefährlichen Rest der Bedrohungen konzentrieren. Ein drittes Element im Zusammenspiel der Endpoint-Schutzlösungen ist Sandboxing. Dabei überprüft Kaspersky Sandbox verdächtige Dateien in einer abgeschotteten Umgebung und meldet die Resultate an die EPP zurück.

EDR erkennt moderne Bedrohungen sofort bei ihrer Ausführung und stoppt den Angriff, noch bevor tiefergehende Schäden in der IT-Infrastruktur entstehen.

Endpoint Detection and Response: die Vorteile

- Kürzere Zeit bis zur Abwehr (MTTR) – entscheidend bei Ransomware-Attacken
- Hoher Automatisierungsgrad entlastet die IT-Security-Abteilung
- Volle Transparenz über die Vorgänge an den Endgeräten
- Detaillierte Vorfallsdaten und unverzügliche Behandlung von Vorfällen
- Keine zusätzlichen Fachkräfte und Schulungen nötig
- Keine gefährlichen Überbleibsel von Angriffen

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch