SOPHOS
Security made simple.

NEXIO
OPERATIONAL IT-SERVICES

Endpoint Exploit Prevention

Stoppen Sie Ransomware – mit den leistungsstarken Funktionen von CryptoGuard

Die Anti-Ransomware- und Anti-Exploit-Funktionen von Sophos Intercept X sind ab sofort auch für Bereitstellungen von Endpoint Protection verfügbar, bei denen die Richtlinien in der Sophos Enterprise Console verwaltet werden. Mit Endpoint Exploit Prevention stoppen Sie Malware, verhindern die Ausnutzung von Schwachstellen und beseitigen verborgene Malware.

Highlights

- Stoppt Crypto-Ransomware und setzt betroffene Dateien automatisch in den Ursprungszustand zurück
- Exploit Prevention bekämpft Methoden, auf die Angreifer zum Ausnutzen von Software-Schwachstellen zurückgreifen
- Forensische Systembereinigung

Systemvoraussetzungen

- Windows 7 bis Windows 10, 32 Bit oder 64 Bit
- Windows Server 2008R2 und höher
- Sophos Enterprise Console 5.5

Erweitern Sie Ihre Endpoint-Protection-Bereitstellung noch heute um Endpoint Exploit Prevention.
Wenden Sie sich an Ihren Sophos-Partner oder besuchen Sie www.sophos.de/endpoint

Ransomware rechtzeitig stoppen

Die bewährten CryptoGuard-Funktionen von Sophos Intercept X kommen nun in unserer Endpoint Exploit Prevention zum Einsatz. Die Technologie blockiert Ransomware, sobald diese versucht, Ihre Dateien zu verschlüsseln, und setzt Daten in ihren Ursprungszustand zurück.

- Macht die Schutztechnologie von Intercept X für Endpoints verfügbar, die über die Enterprise Console verwaltet werden
- Schützt Endpoints vor Ransomware-Angriffen
- Setzt verschlüsselte Dateien automatisch in ihren Ursprungszustand zurück
- Stoppt sowohl lokale Festplatten- als auch Remote-Netzlaufwerkverschlüsselungen

Effektive Abwehr von Exploit-Verfahren

Unsere Anti-Exploit-Technologie erkennt und blockiert gängige Malware-Übertragungsmethoden. So werden Bedrohungen gestoppt, bevor sie zum Problem werden. Dieser Prozess schützt Ihre Endpoints vor Exploit-Kits und schädlichen Payloads, die versuchen, bekannte und unbekannte Software-Schwachstellen auszunutzen.

Erweiterte Bedrohungsbereinigung

Bei der Beseitigung von Malware reicht es nicht mehr, Schadelemente in die Quarantäne zu verschieben und zu löschen. Denn wie können Sie sicher sein, dass auf einem Endpoint erkannte Malware keinen Schaden auf dem betroffenen System angerichtet hat, bevor sie gestoppt wurde? Sophos Clean wird parallel zu unserer Endpoint Exploit Prevention bereitgestellt. So können Sie nach Überresten von Malware scannen und eine gründliche Systembereinigung vornehmen. Sophos Clean erkennt unerwartete Änderungen an Ihrem System. Die Lösung erfasst und entfernt Spuren von Malware, die von herkömmlichen Tools zur Malware- und Virenentfernung oft nicht beseitigt werden.

Verwaltung über die Sophos Enterprise Console

Bestandskunden von Sophos Enpoint Protection, die die Sophos Enterprise Console nutzen, müssen keinen neuen Agenten bereitstellen, um Endpoint Exploit Prevention nutzen zu können. Mit der neuen Lizenz eröffnen sich komplett neue Möglichkeiten auf Richtlinienebene und Agenten-Komponenten werden automatisch bereitgestellt. Benötigen Sie neben leistungsstarkem Schutz auch Funktionen zur Ursachenanalyse und Angriffsvisualisierung? Wechseln Sie zu Sophos Intercept X und verwalten Sie Ihre Endpoints über unsere cloudbasierte Plattform Sophos Central.

NEXIO Operational IT-Services GmbH
Am Giener 22, 55268 Nieder-Olm
Germany
Tel.: +49 (0) 6131-90799-60
WEB: www.nexio.de

19.01.2017 DSDE (NP)