Sophos Endpoint Protection

Einfache und leistungsstarke Sicherheit für Ihre Desktop-Umgebung

Mit Sophos Endpoint Protection schützen Sie Ihre Windows-, Mac- und Linux-Systeme vor Malware und weiteren Endpoint-Bedrohungen. Sophos Endpoint Protection kombiniert bewährte Technologien wie Malicious Traffic Detection mit Echtzeit Bedrohungsdaten aus den Sophos Labs, damit Sie Bedrohungen einfach abwehren, erkennen und beseitigen können. Web-, Anwendungs- und Peripheral-Zugriffsrichtlinien begleiten Benutzer überall. Gleichzeitig tauschen Firewall und Endpoints per Security Heartbeat Sicherheitsinformationen aus.

Grundlegende Funktionen

Anti-Malware/Antivirus: Erkennung bekannter Malware auf Signaturbasis. Malware-Engines sollten nicht nur ausführbare Dateien, sondern auch z. B. schädlichen Javascript-Code auf Websites überprüfen können.

Application Lockdown: Abwehr von schädlichen Verhaltensweisen von Anwendungen: Ein modifiziertes Office-Dokument installiert beispielsweise eine Anwendung und führt diese aus.

Verhaltensüberwachung/Host Intrusion Prevention Systems (HIPS): Diese grundlegende Technologie schützt Computer vor unbekannten Viren und verdächtigem Verhalten. Sie sollte Verhaltensanalysen sowohl vor Ausführung als auch während der Laufzeit beinhalten.

Web Protection: URL-Abruf und Blockierung von bekannten Schadseiten. Zu den blockierten Websites sollten Seiten gehören, die JavaScript-Code ausführen könnten (Cryptomining), und Seiten, die Benutzer-Authentifizierungsinformationen und andere sensible Daten stehlen.

Web Control: Mit Endpoint Web Filtering können Administratoren festlegen, welche Dateitypen ein Benutzer aus dem Internet herunterladen kann.

Data Loss Prevention (DLP): Wird ein Angriff zunächst nicht bemerkt, kann dank DLP die letzte Phase mancher Angriffe erkannt und abgewehrt werden, wenn der Angreifer versucht, Daten abzuschöpfen. Hierbei werden eine Reihe sensibler Datentypen überwacht.

Moderne Funktionen

Machine Learning: Es gibt unterschiedliche Arten von Machine Learning, wie etwa neuronale Deep-LearningNetzwerke, Random Forest, Bayessche Netze sowie Clustering. Machine-Learning-Engines zur Erkennung von Malware müssen in jedem Fall bekannte und unbekannte Malware ohne Rückgriff auf Signaturen erkennen. Der Vorteil von Machine Learning ist, dass sich damit auch bisher unbekannte Malware erkennen lässt, was die Malware-Erkennungsrate erhöht. Unternehmen sollten auf die Erkennungsleistung, False Positive-Raten sowie mögliche Performance-Einbußen von Lösungen auf der Basis von Machine Learning achten.

Anti-Exploit: Anti-Exploit-Funktionen wehren die Tools und Techniken ab, die sich Hacker bei Angriffen zunutze machen. So wurde die Ransomware WannaCry und NotPetya etwa über Exploits wie EternalBlue und DoublePulsar ausgeführt. Anti-Exploit-Technologie stoppt die verhältnismäßig geringe Anzahl an Techniken zur Verbreitung von Malware und Durchführung von Hacker-Angriffen. Dadurch lassen sich zahlreiche bisher unbekannte Zero-Day-Angriffe abwehren.

Spezieller Schutz vor Ransomware: Manche Lösungen beinhalten Funktionen, um die unbefugte Verschlüsselung von Daten durch Ransomware zu verhindern. Häufig werden betroffene Dateien durch diese Anti-Ransomware-Technologie wieder in ihren Ursprungszustand versetzt. Allerdings sollten sich AntiRansomware-Lösungen nicht nur auf Dateien abzielende Ransomware beschränken, sondern auch FestplattenRansomware abwehren, die den Master Boot Record durch zerstörerische Löschangriffe schädigt.

SOPHOS

Credential Theft Protection: Diese Technologie verhindert den Diebstahl von Authentifizierungspasswörtern und Hash-Informationen aus dem Speicher, von der Registry oder der Festplatte.

Process Protection (Privilege Escalation): Schutz, der explizit nach Prozessen sucht, in die zur Ausweitung der Berechtigungen ein privilegierter Authentifizierungstoken im Rahmen eines aktiven Angriffs eingebunden wurde. Unabhängig davon, welche Schwachstelle (bekannt oder unbekannt) ursprünglich zum Diebstahl des Authentifizierungstokens ausgenutzt wurde, sollte dies ein wirksamer Schutz sein.

Sophos Endpoint Protection

Process Protection (Code Cave): Abwehr von Techniken wie Code Cave und AtomBombing, die häufig bei Angriffen eingesetzt werden, die das Vorhandensein seriöser Anwendungen ausnutzen. Angreifer können diese Calls manipulieren und so andere Prozesse dazu bringen, ihren Code auszuführen.

Endpoint Detection and Response (EDR): EDR-Lösungen sollten in der Lage sein, detaillierte Informationen für die gezielte Suche nach evasiven Bedrohungen zu liefern, damit die Durchsetzung von Sicherheitsvorgaben gewahrt bleibt und erkannte Vorfälle zuverlässig analysiert werden können. Es ist wichtig, die Komplexität und Benutzerfreundlichkeit der Lösung Ihrer Wahl auf die Größe und den Spezialisierungsgrad Ihrer Abteilung abzustimmen. Wählen Sie beispielsweise eine Lösung aus, die detaillierte Informationen und Handlungsempfehlungen zu Bedrohungen bietet, damit Sie schnell und einfach auf Bedrohungen reagieren können.

Reaktion auf Vorfälle/Synchronized Security: Endpoint-Tools sollten zumindest Aufschlüsse über die Ursache von Vorfällen bieten, damit weiteren Vorfällen vorgebeugt werden kann. Im Idealfall reagiert die Lösung automatisch – ganz ohne Benutzerzugriff – auf Vorfälle. So können sich Bedrohungen nicht ausbreiten und noch mehr Schaden anrichten. Dabei müssen Tools, die auf Vorfälle reagieren, mit anderen Endpoint- und Netzwerk-Sicherheitstools kommunizieren.

Managed Threat Response (MTR): MTR bietet Managed Detection and Response als 24/7 Fully-Managed-Service von einem Expertenteam Unsere Analysten reagieren auf potenzielle Bedrohungen, suchen nach „Indicators of Compromise“ und liefern detaillierte Analysen der Ereignisse – was ist wo, wann, wie und warum passiert?

Übersichtliche Gestaltung

Trotz der vielen Features, die Sophos Endpoint Security and Control zu bieten hat, ist die Benutzeroberfläche übersichtlich gestaltet. Die verschiedenen Rechner in einem Netzwerk findet Sophos recht schnell. Auch in die Übersicht der PCs, welche Sophos in einem Netzwerk überwacht, hat sich der Nutzer sehr schnell eingearbeitet und die Einteilung in verschiedene Gruppen und Bereiche verursacht keinerlei Schwierigkeiten. Die Auswahl der verschiedenen Scan-Methoden funktioniert kinderleicht und die Anzeige der jeweiligen Scan-Ergebnisse ist kompakt und leicht verständlich.

Die Vorteile von Sophos liegen auf der Hand: Die Software verfügt über eine Fülle von Features im Vergleich zu Marktbegleitern. Es ist mit Sophos nicht nur möglich, die Rechner eines ganzen Netzwerks zu überwachen, der User kann auch für jeden einzelnen von ihnen individuelle Richtlinien einrichten, an die sich der Netzwerkteilnehmer zu halten hat. So werden etwa diverse Webseiten auf einzelnen Computern unzugänglich gemacht. Ansonsten hat Sophos vom Phishing-Schutz über P2P- und IM-Schutz bis hin zur eigenen Firewall alles zu bieten, was der Nutzer sich von einem Antiviren-Programm wünschen könnte. Zudem bietet das Programm auch mit dem sogenannten NAC (Network Access Control) optimale Möglichkeiten, die einzelnen Rechner in einem Netzwerk in Bezug auf die Sicherheitsvorkehrungen schnell und effektiv aufeinander abzustimmen.

SOPHOS

Versionsvergleich

		Endpoint Protection				Intercept X	
	SKU	Endpoint Protection Standard	Endpoint Protection Advanced	Endpoint Exploit Prevention	Central Endpoint Protection	Central Intercep X Advanced	Central Intercept X Advanced with DER
Reduktion der Angriffsfläche	Web Security	X	X		X	X	X
	Download Reputation	X	X		X	X	X
	Web Control/Kategoriebasierte URL-Filterung	X	X		X	X	X
	Peripheral Control (z. B. USB)	X	X		X	X	X
	Application Control	X	X		X	X	X
	Client Firewall	X	X				
Abwehr vor Ausführung auf dem Gerät	„Deep Learning“-Malware-Erkennung					X	X
	Anti-Malware-Dateiscans	X	X		X	X	X
	Live Protection	X	X		X	X	X
	Verhaltensanalysen vor Ausführung (HIPS)	X	X		X	X	X
	Blockierung pot. unerwünschter Anwendungen	X	X		X	X	X
	Patch-Analyse		X				
	Data Loss Prevention		X		X	X	X
	Exploit Prevention			X		X	X
Erkennung / Stoppen von Bedrohungen bei Ausführung	Laufzeit-Verhaltensanalyse (HIPS)	X	X		X	X	X
	Malicious Traffic Detection (MTD)		X		X	X	X
	Active Adversary Mitigations					X	X
	Ransomware File Protection (CryptoGuard)			X		X	X
	Disk and Boot Record Protection (WipeGuard)					X	X
	Man-in-the-Browser Protection (Safe Browsing)			X		X	X
Reaktion Analyse und Beseitung	Automatisierte Malware-Entfernung	X	X		X	X	X
	Synchronized Security Heartbeat				X	X	X
	Ursachenanalyse					X	X
	Sophos Clean			X		X	X
	Endpoint Detection & Response (EDR)						X