SOPHOS
Cybersecurity delivered.

Die wichtigsten Mechanismen zum Schutz vor Ransomware: So kann Sophos helfen

Die Bedrohung durch Ransomware wächst. Innerhalb von zwölf Monaten hat sich der Anteil der von Ransomware betroffenen Unternehmen fast verdoppelt (Anstieg von 37 % in 2020 auf 66 % in 2021). Zudem gelingt es Cyberkriminellen immer häufiger, Daten ihrer Opfer zu verschlüsseln: Im vergangenen Jahr war dies bei 65 % der Angriffe der Fall.*

Maßnahmen zur Abwehr von Ransomware müssen sowohl vor komplexen, manuell gesteuerten Angriffen schützen als auch vor dem beliebten Geschäftsmodell Ransomware-as-a-Service. Dieses erhöht die Reichweite von Ransomware erheblich, da weniger Know-how zur Durchführung eines Angriffs erforderlich ist.

In diesem Guide stellen wir Ihnen die wichtigsten Mechanismen vor, um das Risiko und die Folgen von Ransomware zu minimieren. Außerdem erfahren Sie, wie Sophos dabei helfen kann.

Sophos Solution Brief. April 2022

Die wichtigsten Mechanismen zum Schutz vor Ransomware: So kann Sophos helfen

SCHUTZMECHANISMUS	UNTERSTÜTZUNG DURCH SOPHOS	DETAILS
Proaktives Threat Hunting und Abwehr manuell gesteuerter Angriffe, bevor die Angreifer die Ransomware bereitstellen können	Sophos XDR (Extended Detection and Response)	Ermöglicht Unternehmen, Bedrohungen in ihrer gesamten Umgebung zu erkennen und zu bekämpfen. Erkennungen können von Endpoints, Servern, Cloud-Workloads, der Firewall, E-Mails, Public-Cloud-Umgebungen, Mobilgeräten, Microsoft 365 und mehr stammen.
	Sophos MTR (Managed Threat Response)	24/7/365 Managed Detection and Response mit Threat Hunting durch ein Sophos-Expertenteam, als Fully-Managed-Service. Connectors zu einer Reihe von Security- und IT-Lösungen, einschließlich Microsoft 365, bieten Transparenz über die gesamte Kundenumgebung. So können unsere Analysten Angriffe noch besser abwehren.
Automatisches Blockieren von Ransomware, bevor sie bereitgestellt werden kann	Sophos Endpoint Protection und Sophos Workload Protection	Bietet modernste Schutzfunktionen, die die gesamte Ransomware-Angriffskette stören, einschließlich: › Deep Learning mit künstlicher Intelligenz zur Abwehr bekannter und unbekannter Ransomware. › Exploit-Schutz zum Blockieren von Exploits und Techniken, die zur Verbreitung von Malware, zum Diebstahl von Zugangsdaten und zur Verschleierung von Angriffen eingesetzt werden. › Application Control, um zu verhindern, dass unbefugte Anwendungen in Cloud-Workloads laufen und Cyberkriminelle so Angriffe starten können. › Server Lockdown zum Anwenden und Sperren einer bekanntermaßen sicheren Konfiguration für Cloud-Workloads und Anwendungen, um nicht autorisierte Änderungen zu verhindern. › Anti-Ransomware-Technologie, die unbefugte Verschlüsselungsprozesse erkennt und rückgängig macht, bevor sie sich im Netzwerk ausbreiten können. Schützt sowohl vor dateibasierter als auch Master-Boot-Record-Ransomware.
	Sophos Email	Analysiert automatisch alle Dateiprozesse, Datei- und Registry-Aktivitäten sowie Netzwerkverbindungen, um Ransomware und andere Formen von Malware zu blockieren. Modernster Phishing-Schutz, URL-Scans und Schutz nach der Zustellung stellen sicher, dass nur E-Mails sicherer Absender Ihren Posteingang erreichen. Wenn sich der Bedrohungsstatus von Nachrichten nach der Zustellung ändert, werden die Nachrichten automatisch entfernt.
	Sophos Firewall	Schützt vor kompromittierten Websites und schädlichen Downloads dank ausführlicher Analysen auf Basis von Machine Learning und Sandboxing-Inspektion auf Datei-Downloads. So lassen sich selbst bisher unbekannte Ransomware-Angriffe erkennen.

Die wichtigsten Mechanismen zum Schutz vor Ransomware: So kann Sophos helfen

SCHUTZMECHANISMUS	UNTERSTÜTZUNG DURCH SOPHOS	DETAILS
Ermitteln und Schließen von Sicherheitslücken zum Härten Ihrer Umgebung. Hierzu zählen etwa ungepatchte Geräte, nicht geschützte Systeme und mehr.	Sophos XDR (Extended Detection and Response)	Ermittelt veraltete bzw. nicht unterstützte Software und Systeme. Liefert Zugriff auf alle Anwendungen auf dem Gerät, Versionsinfos, SHA256-Datei-Hashes, Patch-Informationen und Protokolle, einschließlich Ausführungsverlauf der Anwendungen, Netzwerkverbindungen, übergeordnete und untergeordnete Prozesse usw. Umfasst Abfragen zum Abgleich installierter Anwendungen mit Informationen zu Online-Schwachstellen sowie Abfragen zum Ermitteln von Schwächen des Sicherheitsstatus in Registry-Einstellungen.
	Sophos ZTNA (Zero Trust Network Access)	Bietet sicheren, feinstufigen Remote-Zugriff auf Systeme und Anwendungen und reduziert die Angriffsfläche sowie laterale Bewegungen von Angreifern.
Sperren des Remote Desktop Protocols, damit Cyberkriminelle nicht darüber Zugriff erlangen können	Sophos Firewall	Ermöglicht es IT-Teams, das RDP einfach zu verwalten und zu sperren.
	Sophos ZTNA (Zero Trust Network Access)	Bietet sicheren Zugriff auf das RDP und andere Anwendungen und schützt diese Systeme so vor Angriffen.
	Sophos Cloud Optix	Erkennt proaktiv ungeschützte RDP-Ports mit Hilfe von Benchmark-Assessments für Public-Cloud-Sicherheit. Geführte Bereinigungsmaßnahmen helfen Administratoren dabei, fehlerhafte Sicherheitskonfigurationen zu beheben.
	Sophos XDR (Extended Detection and Response)	Erkennt RDP-Verbindungen und protokolliert die Aktivität. Per Remote-Terminal-Zugriff können Administratoren die RDP-Richtlinie aktivieren/deaktivieren. Sorgt für Transparenz über die RDP-Richtlinie auf allen verwalteten Geräten und erkennt Richtlinienänderungen.
Incident-Response-Pläne zur Minimierung der Schäden bei einem Vorfall	Sophos Rapid Response	Bietet bei Vorfällen 24/7-Soforthilfe durch ein Sophos-Expertenteam.
	Sophos MTR (Managed Threat Response)	Bietet 24/7 Managed Detection and Response mit Threat Hunting durch ein Expertenteam, als Fully-Managed-Service.

SCHUTZMECHANISMUS	UNTERSTÜTZUNG DURCH SOPHOS	DETAILS
Cybersecurity-Awareness-Trainings und Phishing-Tests	Sophos Phish Threat	Erhöht das Sicherheitsbewusstsein und schult Benutzer durch Phishing-Angriffssimulationen, automatisierte Security-Awareness-Trainings sowie aussagekräftige Reports. Dank der Integration mit Sophos Email können Security-Teams effizient Benutzer identifizieren und schulen, die gewarnt oder daran gehindert wurden, eine Website mit einem hohen Risikoprofil aufzurufen.
Erkennen und Beheben von Sicherheitslücken in Cloud-Umgebungen, damit sie nicht von Angreifern ausgenutzt werden können	Sophos Cloud Optix	Erkennt und behebt proaktiv Sicherheitslücken, überprivilegierte IAM-Rollen und Konfigurationsfehler beim Netzwerkzugriff in Public-Cloud-Umgebungen mit Integration des Amazon Inspector – einschließlich über das Internet zugänglicher Ports auf virtuellen Maschinen, aktivierter Remote-Root-Anmeldung sowie Installationen anfälliger Softwareversionen. Empfängt den Patch-Status von virtuellen Amazon-Maschinen mit Integration des AWS Systems Manager. Weitet Sicherheitsscans mit Infrastructure-as-Code-Scans auf CI/CD-Pipelines aus und analysiert Container-Registrys in Azure, AWS und Docker Hub auf Schwachstellen im Betriebssystem.

Sie möchten Ihre Cybersecurity zur Abwehr von Ransomware optimieren? Unsere zertifizierten Sophos-Vertriebspartner beraten und unterstützen Sie gerne. Alternativ können Sie auch unser internes Vertriebsteam unter sales@sophos.de kontaktieren.

** Ransomware-Report 2022, Sophos, Befragung von 5.600 IT-Experten in 31 Ländern*

Erfahren Sie mehr über Ransomware und darüber, wie Sophos Sie und Ihr Unternehmen davor schützen kann.

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen, wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2022-04-08 (SB-NP)

SOPHOS