Zero Trust:
Was verbirgt sich dahinter?

Wie stellen Sie Ihr Unternehmen nach der Zero Trust Maßgabe auf ?

Diese Schritte müssen Sie gehen, um Ihr Unternehmen auf Zero Trust umzustellen.

SOPHOS

Security made simple.

CMS, Sudhaus & Partner
Unternehmensberatung GmbH

Unternehmensnetzwerke nach außen abzuschirmen, galt bisher als wirksamstes Sicherheitskonzept. Dieser perimeterbasierte Ansatz funktioniert jedoch immer weniger. Mitarbeiter arbeiten immer öfter mobil, auch über andere Netzwerke. Hinzu kommen Software-as-a-Service-Anwendungen (SaaS), Cloud-Plattformen und cloudbasierte Services. Es gibt nicht mehr das eine Unternehmensnetzwerk, in dem alle darin eingebundenen Systeme sicher sind. Die Grenzen zwischen Innen und Außen verschwimmen zunehmend.

Hier kommt Zero Trust ins Spiel. Zero Trust fußt auf dem Prinzip: „Nichts und niemandem vertrauen, alles überprüfen". Für Zero Trust gibt es nicht den einen Anbieter, das eine Produkt oder die eine Technologie. Vielmehr ist eine Kombination unterschiedlicher Lösungen erforderlich.

In diesem Whitepaper erfahren Sie, was genau sich hinter Zero Trust verbirgt, welche Vorteile die Implementierung eines entsprechenden Modells bietet und welche Schritte zur Umstellung auf Zero Trust notwendig sind.

INHALTSVERZEICHNIS

DIE ZEITEN HABEN SICH GEÄNDERT

Vertrauen ist menschlich, doch in der IT-Security weitgehend fehl am Platz – insbesondere wenn dieses vorbehaltlos und uneingeschränkt gewährt wird.

Hermetisch abgeriegelte Unternehmensnetzwerke, hinter deren Mauern allem und jedem vertraut wird, haben sich immer wieder als fehlerhafte Abwehrstrategie erwiesen. Denn sobald es Hackern gelingt, ins Innere solcher Netzwerke vorzudringen, haben sie leichtes Spiel und können häufig unbemerkt agieren. So können sie sich leicht im Netzwerk ausbreiten, auf wichtige Systeme zugreifen und weiteren Schaden anrichten. Denn die Sicherheitskontrollen und genaue Prüfungen finden nur auf Perimeter-Ebene statt.

Im Klartext heißt das: Traditionelle Netzwerkgrenzen gehören der Vergangenheit an.

Anwender möchten von überall aus arbeiten und sich auch über nicht vertrauenswürdige Netzwerke, wie öffentliche WLANs im Café um die Ecke, einwählen können. Sie möchten ihre Daten in der Cloud speichern, damit sie jederzeit darauf zugreifen können. Auch der Zugang zu Unternehmensdaten und -ressourcen über private Geräte muss gewährleistet sein, damit alle Mitarbeiter ortsunabhängig und zeitlich flexibel arbeiten können.

Durch die Verwendung von SaaS-Anwendungen, Cloud-Plattformen und anderen cloudbasierten Services befinden sich wichtige Daten nun oft außerhalb des Unternehmensnetzwerks. Hinzu kommt, dass viele Geräte und Services extern betrieben werden. Ein weiterer Trend: Workloads werden dorthin verlagert, wo sie sich am kostengünstigsten verarbeiten lassen. Dadurch verlassen sie jedoch unsere eigenen Netzwerke, die wir kontrollieren können.

Alles ist überall. Das alte „Sicherheitsmodell“ mit statischen Schutzmechanismen scheitert an der Aufgabe, Unternehmen die Nutzung neuer Technologien wie der Cloud zu ermöglichen und gleichzeitig ihre Daten, Anwender und Kunden zu schützen. Es ist Zeit umzudenken.

ZEIT FÜR ZERO TRUST

Zero Trust ist ein ganzheitliches Sicherheitskonzept, das auf die neuen Herausforderungen und Arbeitsweisen von Unternehmen eingeht. Es handelt sich um eine Security-Philosophie und -Architektur zur Herangehensweise an das Thema IT-Sicherheit in Unternehmen.

Nichts und niemandem darf automatisch vertraut werden, ob innerhalb oder außerhalb des Unternehmensnetzwerks, noch nicht einmal dem Netzwerk selbst. Bedingungsloses Vertrauen auf Basis des Netzwerkstandorts mit statischen Abwehrmechanismen wie einer herkömmlichen Firewall ist zu riskant geworden.

Kein Vertrauen ist aber auch keine Lösung. Mit Zero Trust ist das Vertrauen temporär. Es wird dynamisch aus weit mehr Datenquellen ermittelt als je zuvor und ständig neu bewertet. Bei den Datenquellen handelt es sich um Informationen über die Zugriffsanfrage selbst, Benutzerdaten, Systeminformationen, Angaben zu Zugangsvoraussetzungen und Bedrohungsanalysen. Darüber hinaus wird der Zugriff auf Daten und/oder Ressourcen nur nach Bedarf pro Verbindung gewährt.

Durch unsere tägliche Nutzung des Internets haben wir ständig mit nicht vertrauenswürdigen Netzwerken zu tun. Dies wiederum bedeutet, dass Computer, die mit dem öffentlichen Internet verbunden sind, ganz anders geschützt werden müssen als solche innerhalb traditioneller Netzwerkgrenzen.
Zur Abwehr externer Bedrohungen sind zusätzliche Kontrollen und mehrschichtige Schutzmaßnahmen erforderlich.

Beim Zero Trust-Modell werden alle Geräte so eingestuft, als wären sie mit dem Internet verbunden. Statt einer einzigen Netzwerkgrenze, gibt es jetzt viele Mikroperimeter (oder Mikrosegmente). Dabei wird der gesamte Netzwerkverkehr umfassend kontrolliert.

DIE VORTEILE VON ZERO TRUST IM ÜBERBLICK

Die Implementierung eines Zero-Trust-Modells bringt unzählige Vorteile, u. a:

Kontrolle über die gesamte IT-Umgebung

Von Ihrem Büro bis zu den von Ihnen verwendeten Cloud-Plattformen: Sie müssen sich keine Gedanken mehr über einen eventuellen Kontrollverlust außerhalb des Unternehmensnetzwerks machen und können Mitarbeitern außerhalb des Büros genauso einfach Zugriff erteilen wie Mitarbeitern im Büro.

Gleichbehandlung aller Anwender

Wenn Sie nicht mehr zwischen innerhalb und außerhalb des Unternehmensnetzwerks unterscheiden, können Sie alle Anwender auf die gleiche Weise behandeln. Dadurch wird es einfacher, für die notwendige IT-Sicherheit zu sorgen und gleichzeitig sicherzustellen, dass alle Geräte und Anwender gleich behandelt werden.

Maximale Sicherheit für Ihre Infrastrukturen

Durch die Verwendung von Identität, Standort, Integritätsstatus des Geräts, MFA und übergreifender Überwachung und Analyse können Sie stets ein hohes Maß an Sicherheit gewährleisten – unabhängig von Umgebung, Plattform oder Service.

Effektiver Schutz gegen Malware und Angreifer

Mit Zero Trust haben Angreifer nach einem erfolgreichem Eindringen nicht mehr Zugriff auf das gesamte Netzwerk. Sie können stattdessen nur noch auf eine sehr geringe Anzahl von Systemen zugreifen, auf die der kompromittierte Anwender Zugriff hatte. Auch die Vertrauenswürdigkeit von authentifizierten Anwendern wird weiterhin ständig hinterfragt. So schränkt die Überprüfung zwischen den einzelnen Systemen eine unerwünschte Verbreitung weiter ein.

ZERO TRUST AUF DEN PUNKT GEBRACHT

Es gibt kein „innerhalb“ des Netzwerks

Nichts und niemandem vertrauen, alles überprüfen

IT-Sicherheit sollte sich in Echtzeit anpassen

Zero Trust ist ein weitreichendes Konzept, das für jede Menge Gesprächsstoff sorgt. Im Wesentlichen sind es jedoch diese drei Schlüsselaspekte, die Sie bei Ihrem schrittweisen Rollout von Zero Trust berücksichtigen sollten.

Es gibt kein „innerhalb“ des Netzwerks

Stellen Sie sich vor, Sie würden Ihr gesamtes Unternehmen von einem nicht vertrauenswürdigen Standort aus steuern, z. B. über das öffentliche WLAN eines Cafés, und sämtliche Geräte wären direkt mit dem unsichersten Netz aller Netze verbunden: dem öffentlichen Internet. In einer solchen Situation können Sie sich nicht auf die „schützenden Mauern“ einer klassischen Netzwerkgrenze verlassen und müssen Ihr komplettes Sicherheitskonzept überdenken.

Es wird immer „vertrauenswürdige“ Unternehmensnetzwerke für administrative und interne Systeme geben. Das Ziel ist jedoch, den Endanwender durch Einsatz von Anwendungsproxys und weiteren Technologien von diesen Netzwerken fernzuhalten, um so die Angriffsfläche drastisch zu reduzieren.

Nichts und niemandem vertrauen, alles überprüfen

Gehen Sie davon aus, dass es sowohl innerhalb als auch außerhalb Ihrer Netzwerke Hacker gibt, die immer präsent sind und ständig angreifen. Kein Anwender oder Gerät darf automatisch als vertrauenswürdig eingestuft werden und muss sich authentifizieren, bevor eine Verbindung überhaupt in Betracht gezogen werden kann. Wenn Sie ständig damit rechnen müssen, von allen Seiten angegriffen zu werden, sind Sie quasi dazu gezwungen, eine solide Authentifizierung und Autorisierung für Ihre Ressourcen zu erstellen. Zudem gilt es, mehrere Schutzschichten zu implementieren und alle Vorgänge in Ihrer Umgebung kontinuierlich zu überwachen und zu analysieren.

IT-Sicherheit sollte sich in Echtzeit anpassen

Die Sicherheitsrichtlinien, die Sie im Rahmen von Zero Trust einführen, sollten dynamisch sein und sich automatisch anpassen. Die dazu notwendigen Erkenntnisse lassen sich anhand von möglichst vielen Datenquellen und unterschiedlichen Technologien ermitteln. Eine statische Richtlinie wie „DIESER BENUTZER“ auf „DIESEM GERÄT“ kann auf „DIESE SACHE“ zugreifen, schützt Sie nicht, wenn das Gerät kompromittiert wird, während der Anwender dieses nutzt. Wenn Ihre Richtlinie jedoch auch den Integritätsstatus des Geräts berücksichtigt, z. B. die Identifizierung schädlicher Verhaltensweisen, kann entsprechend reagiert werden, ohne dass ein Administrator aktiv werden muss.

Dieser wichtige Aspekt ist bereits seit Langem Teil der Strategie und Cybersecurity-Philosophie von Sophos. Sie kennen dieses Konzept vielleicht als Synchronized Security, bei der unsere Produkte Sicherheitsinformationen untereinander austauschen und damit für einzigartige Transparenz sorgen. Das Ergebnis: anpassungsfähige, dynamische Richtlinien, die niemals statisch sind und somit nicht leicht umgangen werden können.

Bei einem Großteil davon handelt es sich schlicht und einfach um bewährte Sicherheitsverfahren, die Sie u. U. schon längst anwenden. Und wenn Sie zwischenzeitlich Vorkehrungen zur Einhaltung der DSGVO getroffen haben, ist vieles bereits vorhanden.

ZERO-TRUST-PRINZIPIEN

Nichts ist vertrauenswürdig. Niemals. Wenn Sie nichts und niemandem vertrauen, sind Sie gezwungen, überall dort, wo ein Risiko besteht, relevante Sicherheitsmaßnahmen zu ergreifen.

Alles überprüfen: Gehen Sie nicht automatisch davon aus, dass ein Anwender mit Zugangsdaten vertrauenswürdig ist. Es bedeutet lediglich, dass er im Besitz der Zugangsdaten ist. Sie könnten auch gestohlen sein.

Daraus ergeben sich vier einfache Prinzipien, die es zu berücksichtigen gilt:

Immer identifizieren

Sie benötigen eine zentrale autorisierende Identitätsquelle, die Sie in Ihrer gesamten Umgebung mit Single-Sign-On (SSO) verwenden. Alles sollte mittels mehrstufiger Authentifizierung (MFA) überprüft werden. Unabhängig davon, wo sich der Anwender befindet und worauf er zugreifen möchte: Prüfen Sie seine Zugangsdaten, seinen zweiten (oder dritten) Faktor und fordern Sie regelmäßig eine erneute Authentifizierung an.

Handelt es sich um gestohlene Zugangsdaten oder um System-Manipulationen, bereiten MFA und regelmäßige Neuauthentifizierungen dem Treiben schnell ein Ende.

Immer kontrollieren

Wenden Sie überall dort Kontroll- und Prüfmechanismen an, wo sie benötigt werden, und weisen Sie jeweils nur die Rechte zu, die ein Anwender zur Erledigung seiner Aufgaben benötigt. Wenn es beispielsweise ein Personalsystem gibt, das nur von in Deutschland ansässigen Mitarbeitern genutzt wird, dann sollte ausschließlich die in Deutschland ansässige Belegschaft Zugriff haben. Niemand sonst sollte auf das System zugreifen können, auch bei geringem Risikopotenzial.

Immer analysieren

Nur weil eine Authentifizierung erfolgreich war oder dem Anwender oder Gerät Zugriff gewährt wird, lässt dies keine Rückschlüsse auf die Vertrauenswürdigkeit zu. Denn Insider mit böswilligen Absichten oder Cyberkriminelle können sich möglicherweise Zugriff auf gültige Zugangsdaten verschaffen. Zeichnen Sie alle Netzwerk- und Systemaktivitäten auf und analysieren Sie diese regelmäßig, um zu überprüfen, was nach der Authentifizierung geschieht. SIEMs (Security Information and Event Management), EDR (Endpoint Detection and Response) sowie MDR (Managed Detection and Response) wurden für genau diesen Zweck entwickelt.

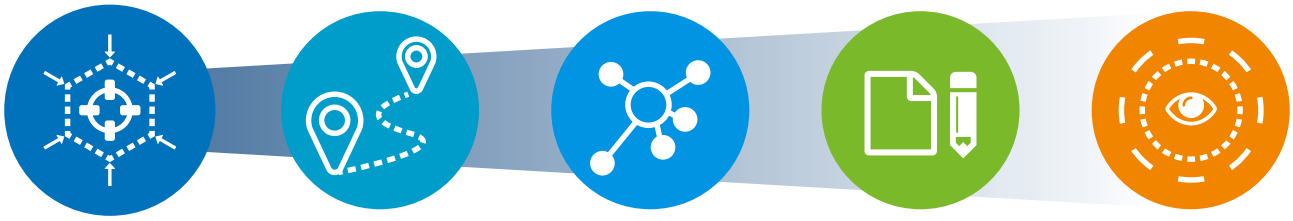
Immer schützen

Setzen Sie bei der Cybersecurity auf einen „Inside-Out"-Ansatz. Das heißt: Sie nehmen Ihre wichtigen Daten als Ausgangspunkt und identifizieren Schwachstellen entlang der Bewegungen Ihrer Daten im Netzwerk – von der Erstellung bis zur Vernichtung der Daten.

Dabei haben Risiken stets Priorität, nicht Compliance oder Vorschriften. Sicherheitsmaßnahmen ausschließlich anzuwenden, um Compliance-Anforderungen oder Vorschriften zu erfüllen, ist gefährlich. Denn was sich in Ihrem Netzwerk befindet oder welche Abläufe, Workloads, Systeme und Technologien ausgeführt werden, kann nicht per Compliance erfasst werden. Auch nicht die Risiken, die für jedes potenzielle Element Ihres Netzwerks relevant sind. Indem Sie mögliche Risiken berücksichtigen und entsprechende Bedrohungsszenarien modellieren, können Sie die Sicherheitsmaßnahmen in bestimmten Bereichen gezielt verschärfen, lockern oder bei Bedarf Mikrosegmente erstellen.

UMSTELLUNG AUF ZERO TRUST

Wie können Sie auf Zero Trust umstellen und alle damit verbundenen Vorteile nutzen?



Definieren Sie Ihre Oberfläche und identifizieren Sie Ressourcen

Bilden Sie standardisierte und privilegierte Pfade ab

Gestalten Sie Ihr Zero-Trust-Netzwerk

Erstellen Sie Zero-Trust-Richtlinien

Überwachen und sichern Sie Ihre Perimeter

Definieren Sie Ihre Oberfläche und identifizieren Sie Ressourcen

Zunächst müssen Sie festlegen, welche Oberfläche Sie schützen, kontrollieren und überwachen möchten. Welche Ressourcen, Services, Anwendungen und Geräte werden in Ihrem Unternehmen verwendet? Bevor Sie die neue Zero-Trust-Mentalität verankern können, müssen Sie sich einen klaren Überblick über alle im gesamten Netzwerk verwendeten Elemente verschaffen.

Bilden Sie standardisierte und privilegierte Pfade ab

Sobald Sie über einen klaren Lageplan verfügen, geht es mit der Abbildung der Standardpfade weiter – welche Datenflüsse, Verhaltensweisen und Beziehungen sind zwischen den einzelnen Elementen standardmäßig zu erwarten? Diese Benutzergruppe greift auf diese Anwendung zu, dieses Gerät stellt eine Verbindung zu jenem Netzwerk her, dieser Service verwendet diesen Datenspeicher und so weiter. Und wie sieht es mit den privilegierten Pfaden aus? Da möchte beispielsweise ein bestimmter Administrator eine Verbindung zur Management-Konsole herstellen und Remote Desktop Protocol (RDP) verwenden, um auf einen bestimmten Server zuzugreifen, auf dem vertrauliche Daten gehostet werden. Für privilegierte Pfade sind höchstwahrscheinlich zusätzliche Sicherheitsmaßnahmen und Kontrollen erforderlich.

Gestalten Sie Ihr Zero-Trust-Netzwerk

Nach der Bestandsaufnahme sind Sie im Bilde, welche Beziehungen zwischen den einzelnen Elementen bestehen, und können mit der Umsetzung der Zero-Trust-Philosophie beginnen. Legen Sie fest, welche Sicherheitsmaßnahmen und Zugriffskontrollen Sie anwenden möchten, und wo welche Technologie welches Risiko am besten eindämmt.

Erarbeiten Sie Zero-Trust-Richtlinien

Als Nächstes müssen Sie Zero Trust-Richtlinien erstellen und implementieren, die so viele verschiedene Datenquellen wie möglich nutzen, um Kontextbezüge zu jeder Verbindung oder Anfrage einzubinden.

Überwachen und sichern Sie Ihre Perimeter

Im letzten und vielleicht sogar wichtigsten Schritt geht es um die genaue Überwachung sämtlicher Vorgänge, um die neu erstellten Perimeter kontinuierlich zu schützen.

Dies ist wohl eine der tiefgreifendsten Veränderungen, mit der sich Administratoren befassen müssen. Bisher musste lediglich die gewünschte Antivirus-Software installiert und entsprechend konfiguriert werden. Ein Blick in die Konsole war nicht notwendig. Bei Zero Trust sieht das anders aus.

Sie müssen alle Ereignisse im Blick behalten und mit Tools wie EDR ermitteln, warum ein Angreifer in die Umgebung eindringen konnte und welche Ereignisse vor einer Erkennung oder nach einer potenziellen Sicherheitspanne stattfanden.

Services wie MDR können hier sehr hilfreich sein, da sie Cybersecurity-Experten ermöglichen, Sie bei der Überwachung Ihres Netzwerks und der Abwehr von Bedrohungen zu unterstützen.

DAS ZERO-TRUST-TECHNOLOGIEPAKET

Das Zero-Trust-Modell basiert auf einer Kombination unterschiedlicher Technologien, um alle Ressourcen und Assets im Netzwerk zu schützen. Daher gibt es keine schlüsselfertige Lösung, die alle Probleme auf einen Schlag löst.

Ein wirksames Zero-Trust-Technologiepaket muss vor allem zwei Aufgabenbereiche abdecken:
die Verwaltung und Steuerung von Zero Trust sowie die Sicherheit und Kontrolle der verschiedenen Assets und Ressourcen.

Die Verwaltung gliedert sich in drei Teilbereiche:

1. Automatisierung und Orchestrierung – umfasst die Definition dynamischer Richtlinien, die Koordination der unterschiedlichen Technologien sowie die gesamte Umsetzung

2. Transparenz und Analyse – ermöglicht, den Überblick über das Netzwerk zu behalten, den störungsfreien Betrieb sicherzustellen sowie Bedrohungen und Eindringlinge zu identifizieren

3. APIs – sorgen für die Integration verschiedener Technologien und die Übertragung von Daten zwischen Systemen

Ressourcen und Assets gliedern sich in fünf Teilbereiche:

1. Personen – die Anwender, Administratoren usw., die für Ihr Unternehmen arbeiten oder Ihre Dienste in Anspruch nehmen

2. Daten – das Lebenselixier aller Unternehmen und vielleicht das schützenswerteste Asset überhaupt

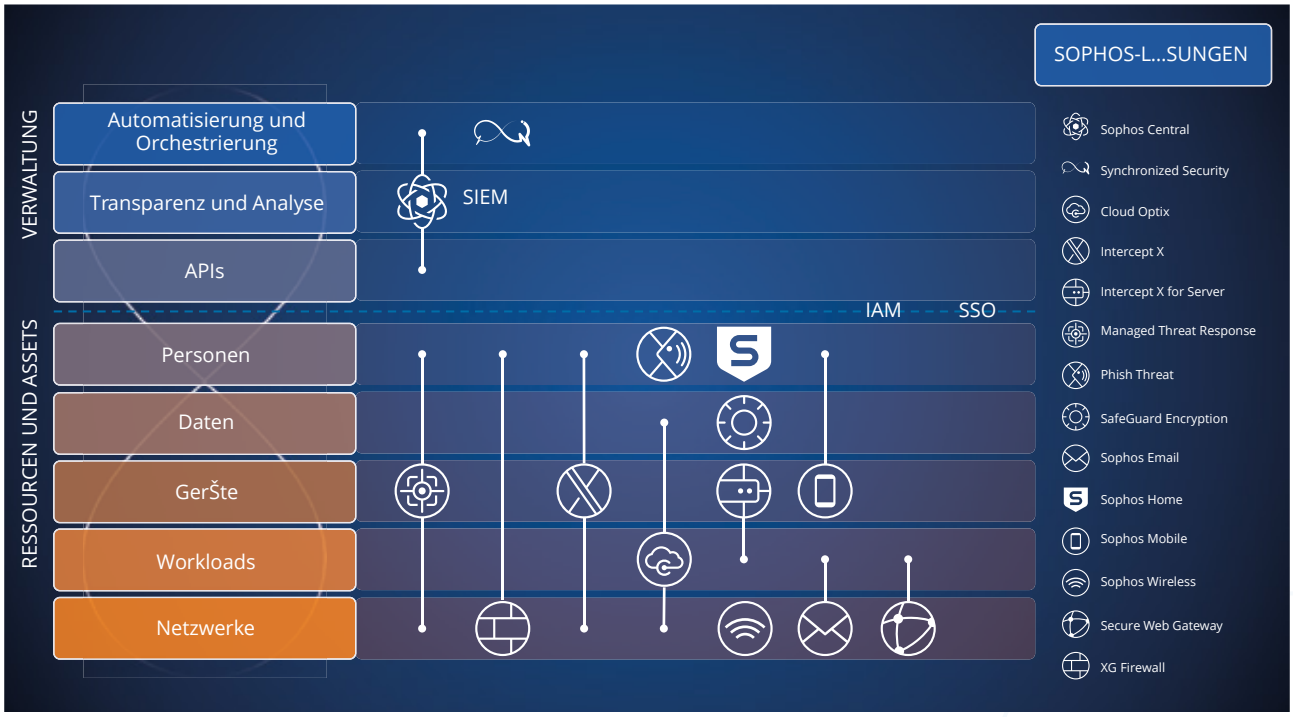
3. Geräte – die Server, Laptops, virtuellen Maschinen usw., die Sie für Ihren Geschäftsbetrieb verwenden

4. Workloads – die Services und Anwendungen, die Sie zur Verarbeitung von Daten, zur Durchführung von Berechnungen, zur Berichterstellung usw. verwenden

5. Netzwerke – die Kommunikationskanäle, über die Daten fließen: Web, E-Mail, WLAN, Internet usw.

WIE CMS, SUDHAUS & PARTNER MIT SOPHOS HELFEN KANN

Es gibt nicht den einen Anbieter, der Ihr Unternehmen auf Zero Trust umstellen kann. CMS hat mit Sophos jedoch ein umfassendes Technologie-Portfolio, das Sie auf dem Weg zu Zero Trust optimal unterstützt. Dabei steht Ihnen CMS Sudhaus als kompetenter Partner im Rahmen der Umstellung in allen Fragen und Belangen zur Verfügung und begleitet Sie auf diesem Weg.



Verwaltung von Zero Trust

Unsere cloudnative Cybersecurity-Plattform **Sophos Central** ermöglicht Ihnen, Ihre Zero-Trust-Umgebung zu verwalten. Sophos Central vereint alle Ihre Technologien in einer Konsole. So haben Sie stets alle Systeme und APIs zur Anbindung von Drittanbieter-Technologien an einem zentralen Ort im Blick.

Eine weitere Option wäre ein SIEM-System, mit dem Sie die Protokollierung von Sophos- und Nicht-Sophos-Produkten zusammenfassen und sich so einen vollständigen Überblick über alle Aktivitäten verschaffen können. Mit unseren APIs können Sie Informationen aus unserer Sophos-Central-Plattform in ein beliebiges SIEM-System Ihrer Wahl übertragen.

Auch **Sophos Synchronized Security** (gesteuert über Sophos Central) spielt hier eine wichtige Rolle. Bei aktivierter Synchronized Security tauschen Sophos-Lösungen untereinander Informationen aus und reagieren automatisch auf Vorfälle. Im Rahmen von Zero Trust sind Lösungen in der Lage, sich durch dynamische Richtlinien an Szenarien anzupassen und komplexe Aufgaben, wie die Isolierung von Systemen, zu automatisieren.

Sicherheit und Kontrolle von Ressourcen und Assets

Viele unserer Produkte helfen Ihnen dabei, mehrere Ressourcen und Assets gleichzeitig zu schützen. Das bedeutet jedoch keinesfalls, dass eine einzige Technologie ausreichend ist und man sich dann entspannt zurücklehnen kann. Für ein ausfallsicheres Netzwerk mit Zero-Trust-Architektur ist das Zusammenspiel mehrerer Technologien erforderlich, um beispielsweise für den Schutz von Personen zu sorgen.

Cloud Optix bietet die kontinuierliche Analyse und Transparenz, die Unternehmen zum Erkennen, Beseitigen und Vorbeugen von Sicherheits- und Compliance-Lücken in der Cloud benötigen. In einer Zero-Trust-Umgebung hilft Cloud Optix, Daten, Geräte, Workloads und Netzwerke innerhalb der Public Cloud zu schützen.

Intercept X bietet einmaligen Endpoint-Schutz und ist in der Lage, mit einer einzigartigen Kombination aus Deep-Learning-Malware-Erkennung, Exploit Prevention, Verhaltenserkennungen und Anti-Ransomware eine besonders große Bandbreite an Angriffen zu stoppen. In einer Zero-Trust-Umgebung sorgt Intercept X für den Schutz aller Ressourcen und Assets.

Intercept X for Server ist speziell für den Schutz von lokalen, hybriden oder Cloud-Serverumgebungen konzipiert. Intercept X for Server sichert in einer Zero-Trust-Umgebung sowohl Ihre Geräte als auch Ihre Workloads.

Managed Threat Response (MTR) ist unsere Threat-Reponse-Lösung aus Expertenhand. Sie kombiniert maschinelles Lernen mit menschlicher Intelligenz und bietet 24/7 Managed Detection and Response mit Threat Hunting. In einer Zero-Trust-Umgebung trägt MTR zum Schutz aller Ressourcen und Assets bei.

Phish Threat ist unsere spezielle Anti-Phishing-Lösung. Sie bietet Ihren Mitarbeitern Security-Awareness-Trainings sowie aussagekräftige Reporting-Daten, die Aufschluss darüber geben, wie gut Ihr Unternehmen gegen Phishing-Bedrohungen gewappnet ist. In einer Zero-Trust-Umgebung trägt Phish Threat zum Schutz Ihrer Mitarbeiter bei.

SafeGuard Encryption verschlüsselt Inhalte direkt nach ihrer Erstellung. Die Lösung schützt Ihre Daten proaktiv, indem sie die Benutzer-, Anwendungs- und Sicherheitsintegrität eines Geräts überprüft, bevor der Zugriff auf verschlüsselte Daten gewährt wird. Dies trägt in einer Zero-Trust-Umgebung erheblich zum Schutz Ihrer Daten bei.

Das **Secure Web Gateway** ermöglicht erweiterten Web-Schutz und bietet ein beispielloses Maß an Web-Sicherheit, -Kontrolle und -Transparenz. In Zero-Trust-Umgebungen bietet das Secure Web Gateway Schutz von Netzwerken und Workloads.

Sophos Email nutzt künstliche Intelligenz für intelligentere prädiktive E-Mail-Security. In Zero-Trust-Umgebungen sorgt Sophos E-Mail für den Schutz von Netzwerken und Workloads.

Sophos Home wurde zum Schutz Ihrer privaten Computer entwickelt und basiert auf der gleichen Technologie, die in vielen unserer Business-Produkte zum Einsatz kommt. In Zero-Trust-Umgebungen sorgt Sophos Home für den Schutz Ihrer Mitarbeiter.

Sophos Mobile ist unsere sichere Unified Endpoint Management (UEM)-Lösung, mit der Unternehmen traditionelle und mobile Endpoints einfacher und zeitsparender verwalten und schützen können. In einer Zero-Trust-Umgebung sorgt Sophos Mobile für den Schutz Ihrer Geräte, Daten und Mitarbeiter.

Mit **Sophos Wireless** verwalten und schützen Sie Ihre WLANs einfach und effizient. In Zero-Trust-Umgebungen trägt Sophos Wireless zum Schutz Ihrer Netzwerke bei.

Die **XG Firewall** bietet umfassenden Next-Generation-Firewall-Schutz, der verborgene Risiken aufdeckt, unbekannte Bedrohungen blockiert und automatisch auf Vorfälle reagiert. In Zero Trust-Umgebungen trägt die XG Firewall zum Schutz aller Ressourcen und Assets bei.

Mit diesen Technologien ist Ihr Unternehmen für den Umstieg auf ein Zero-Trust-Modell gut aufgestellt. Wie bereits erwähnt, kann jedoch kein einzelner Anbieter und keine einzelne Technologie – auch Sophos nicht – die Umstellung auf eine Zero-Trust-Umgebung allein bewerkstelligen. Ein weiterer wichtiger Erfolgsfaktor für Zero Trust ist eine starke IAM-Lösung (Identity Access Management) mit SSO (Single-Sign On), damit Ihre Anwender von jedem beliebigen Standort aus problemlos auf Cloud-Services zugreifen können. Nur so lässt sich Ihre zentrale autorisierende Identitätsquelle für alle Systeme und Services nutzen.

Als zertifizierter Sophos-Partner unterstützt CMS, Sudhaus & Partner Sie bei der Umstellung zu Zero Trust und stellt mit Ihnen die Weichen für eine sichere Zukunft.

Ihr Vorteil als Kunde von CMS, Sudhaus & Partner:

- ✔ **24/7 Kundenservice**
- ✔ **Exklusive Rabattaktionen**
- ✔ **Implementierung und Betreuung aus einer Hand**
- ✔ **Maßgeschneiderte Angebote an Ihre individuellen Bedürfnisse**

Weitere Informationen und sofort abrufbare Demos unserer Produkte und Services finden Sie unter Leistungen auf unserer Webseite:

Klicken Sie hier für weitere Informationen

UNSERE CYBERSECURITY-VISION

Zero Trust und unsere Cybersecurity-Vision „Synchronized Security“ verfolgen vielfach dieselben Ziele und ergänzen sich.

Synchronized Security ist unser innovatives Cybersecurity-System. Es analysiert und automatisiert die komplexesten IT-Aufgaben und passt sich dabei kontinuierlich an. Gleichzeitig werden alle Systemaktivitäten, einschließlich Benutzerverhalten, Netzwerkverkehr und Compliance-Status, dynamisch in Echtzeit überwacht. Alle Technologien kommunizieren miteinander und liefern sich gegenseitig Erkenntnisse und Informationen zu Problemstellen, die nicht durch eine einzige Technologie erkennbar wären.

Nur durch diese Kommunikation sind die für ein Zero-Trust-Netzwerk so entscheidenden dynamischen Richtlinien möglich, die auf einer Vielzahl von Datenquellen basieren.

FAZIT

Bislang ist Zero Trust eine Cybersecurity-Philosophie, die nur sehr wenige Unternehmen ohne Weiteres in die Tat umsetzen können. Da traditionelle Netzwerkgrenzen jedoch zunehmend in Auflösung begriffen sind, wird eine Umstellung auf Zero Trust über kurz oder lang unausweichlich sein. Denn der Einfallsreichtum der Cyberkriminellen scheint keine Grenzen zu kennen. Mit ihrem Tempo können konventionelle Abwehrstrategien kaum Schritt halten. Hier bietet das Zero-Trust-Modell ein zeitgemäßes Sicherheitskonzept, das Bedrohungen entscheidend reduziert und gleichzeitig dazu beiträgt, neue Cybersecurity-Standards zu etablieren.

CMS, SUDHAUS & PARTNER

Boschstraße 1
48703 Stadtlohn
Tel. 0 25 63 - 929 400
www.cms-sudhaus.de