Schützen Sie Ihr Zero-Trust-Datencenter, Ihr wertvollstes Gut

Das Datencenter beherbergt das wertvollste Gut Ihres Unternehmens: Ihre sensibelsten Daten und Anwendungen, ob vor Ort oder in der Cloud. Unabhängig vom Standort ist es von größter Wichtigkeit, dass sie geschützt bleiben. Es ist von entscheidender Bedeutung, die Komponenten des Zero-Trust-Datencenters zu verstehen und zu gewährleisten, dass Sie über die erforderlichen Sicherheitsmaßnahmen verfügen, um Ihre Daten zu schützen und zu bewahren.

Mangelnde Visibilität

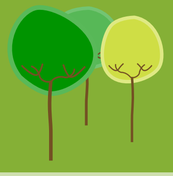
Visibilität im gesamten Netzwerk ist eine Grundvoraussetzung für die kontinuierliche Bewertung des Anwendungs- und Netzwerkzustands und die schnelle Erkennung verdächtiger Aktivitäten. Man kann sich nicht vor dem schützen, was man nicht sieht.

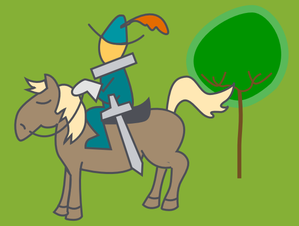
Das wertvollste Gut

Ihre geschäftskritischen und sensiblen Daten und Anwendungen, ob vor Ort oder in der Cloud, sind Ihr wertvollstes Gut. Wenn diese Daten in die falschen Hände geraten, kann das katastrophale Folgen für Ihr Unternehmen haben.

Bedrohungen unterwegs

Bedrohungen werden über viele verschiedene Angriffsvektoren in das Netzwerk eingeschleust und richten sich gegen verschiedene Ziele. Unabhängig von der Absicht oder der eingesetzten Technik ist es wichtig, dass Sie Ihr Datencenter mit den richtigen Tools schützen.





Innerhalb des Datencenters

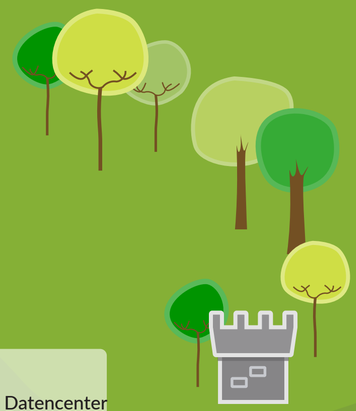
Die Firewall führt zwischen Gruppen von Services und Anwendungen eine weitere Prüfung zwischen Servern mit geschützter Ost-West- und Nord-Süd-Verbindung durch, um sicherzustellen, dass alle Ressourcen und Anwendungen auf verschiedenen Servern nicht gefährdet sind. Wir können festlegen, wie der Datenverkehr zu einer bestimmten Anwendung gelangen kann und auf welche Weise bestimmte Benutzer darauf zugreifen dürfen.

Schutz von Cloud-Workloads

Wir müssen einzelne Anwendungen schützen. Containerisierte Firewalls können für jede Anwendung eingesetzt werden, was einen weiteren Kontrollpunkt darstellt. Wie bei einem Angriff auf die Kronjuwelen muss es bei einem Eindringungsversuch einen Wachposten geben, der den Angriff stoppt. Der Schutz von Cloud-Workloads findet innerhalb der Anwendung selbst statt. Wenn unberechtigt auf die wertvollsten Daten zugegriffen wird, wird der Zugang gesperrt und der Angreifer isoliert und unschädlich gemacht.

Die Vernetzung von Datencentern

Die Vernetzung von Datencentern bildet den Durchgang für die Kommunikation zwischen den Standorten der Datencenter. Die meisten Unternehmen verfügen über mehrere verschiedene Datencenter-Umgebungen. Ein leistungstarker Router ist für den Schutz des Datenverkehrs zwischen Clouds und lokalen Umgebungen unerlässlich. Wenn ein Angreifer sich Zugang zu einem Datencenter verschafft, kann er nicht in alle Standorte eindringen.



Geschäftskontinuität

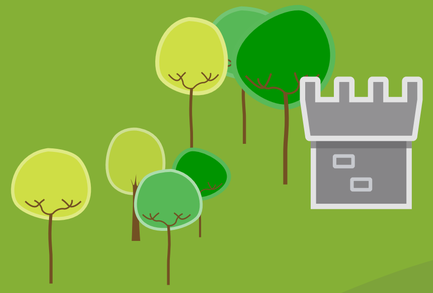
Unternehmen benötigen zuverlässige Verbindungen und müssen die Geschäftskontinuität aufrechterhalten sowie konsistente Sicherheitsrichtlinien mit einem qualitativ hochwertigen Benutzererlebnis und den Zugang zu Services gewährleisten, unabhängig davon, wo sich die Datencenter eines Unternehmens befinden. Die Verwaltung gewährleistet die Sicherheit der Verbindungen zwischen den Datencentern und unterstützt die Orchestrierung und Überwachung von Bereitstellungen an jedem Ort, ob vor Ort oder in der Cloud.

Wenn Ihre Daten angegriffen werden

Was Sie auch tun, es gibt immer Angreifer, die versuchen, Schwachstellen auszunutzen, um an Ihre Daten zu gelangen. Sie müssen vorbereitet sein. Bei der Sicherheit muss im Mittelpunkt stehen, was Sie sehen, was Sie wissen und was Sie tun. Um sichere Datencenter zu schützen, müssen Sie ein auf Bedrohungen vorbereitetes Netzwerk schaffen, indem Sie Visibilität, Intelligenz und die Durchsetzung von Richtlinien auf jeden Verbindungspunkt vom Client bis zum Workload erweitern.

Das WAN-Gateway des Datencenters

Das WAN-Gateway des Datencenters ist der Eingang zum Datencenter und wird durch Firewalls geschützt, die den ein- und ausgehenden Datenverkehr überprüfen und sicherstellen, dass Benutzer und Geräte den richtigen Zugang zum Datencenter erhalten. Wie an einem Sicherheitskontrollpunkt überprüfen wir den eingehenden Datenverkehr, um sicherzustellen, dass sich keine versteckte Malware einschleicht.



DAS AUF BEDROHUNGEN VORBEREITETE NETZWERK FÜR DAS CLOUD-ZEITALTER

Ein Zero-Trust-Datencenter bietet das auf Bedrohungen vorbereitete Netzwerk und verbessert letztendlich die Sicherheit, während es gleichzeitig die Komplexität reduziert und das Management optimiert. Wenn Unternehmen ihr Netzwerk auf Bedrohungen vorbereiten, werden Angriffe früher erkannt und Angreifer haben weniger Chancen, im Netzwerk Fuß zu fassen, wodurch Benutzer, Anwendungen, Infrastruktur und natürlich Ihre wertvollsten Daten geschützt werden.

PN: 3050145