DTS

DTS
Cloud Security

Cloud Security

Cyberangriffe treffen Unternehmen jeder Größe und aus jeder Branche - und täglich werden es mehr: bis zu 144 Millionen neue Malware-Programme pro Jahr, über 390.000 Varianten am Tag, 16.000 Viren oder Trojaner pro Sekunde. Die Zahlen der vergangenen Jahre zeigen eine bedrohliche Entwicklung von Schadsoftware. Zudem steigen im Zuge der fortschreitenden Digitalisierung die Schwachstellen in Programmen kontinuierlich an. Gängige Antivirus-Lösungen und deren Schutzmethoden vor Malware und Exploits sind dieser Herausforderung nicht mehr gewachsen. Mit Cortex XDR Prevent von Palo Alto Networks bieten wir Ihnen eine innovative Sicherheitsstrategie, welche den komplexen Anforderungen gerecht wird.

- Ganzheitliche Absicherung Ihrer Cloud-Umgebung
- Ganzheitliche Betrachtung des Security Stacks
- Individuelle, auf Ihr Unternehmen zugeschnittene Lösungen
- Konzeptionierung, Implementierung, Betrieb & Absicherung in der Cloud
- Über 20 Jahre Know-how mit Cloud-Infrastrukturen
- 24/7 Support in Deutsch & Englisch
- Fokussieren Sie sich auf Ihre Kernkompetenzen mit Hilfe von DTS Managed Services

Das entscheidende Stichwort lautet „Shared Responsibility“, das richtige Verständnis von Verantwortlichkeiten für Applikationen und Daten in der Cloud. Bei der Nutzung der Cloud sind immer beide Parteien, das Unternehmen bzw. der Kunde und der Cloud-Betreiber bzw. Anbieter, für verschiedene Aspekte der Sicherheit verantwortlich. Einzig die ideale Zusammenarbeit beider Parteien ermöglicht einen möglichst vollständigen Schutz. Dabei gibt die Art des genutzten Cloud-Modells grundsätzlich vor, wer für welche Sicherheitsaufgaben verantwortlich ist. Man kann jedoch festhalten, dass die Verantwortlichkeiten des Unternehmens größer sind und tendenziell zunehmen.

Ein sicherer Weg in die Cloud
Moderne Cloud-Sicherheitslösungen unterstützen die Konsolidierung Ihrer Cyberabwehr und fördern die geschäftliche Flexibilität. Die Migration in die Cloud stellt die IT-Sicherheitsexperten von Unternehmen vor zwei wichtige Fragen: Wie können die Benutzer sicheren Zugriff auf die Cloud erhalten? Wie lassen sich in der Cloud gehostete Anwendungen effektiv schützen? Bisher bestand die Antwort auf diese Fragen meist in der Kombination von verschiedenen, voneinander isolierten Punktlösungen. Das bedingt wiederum Mehrkosten und zusätzliche Komplexität sowie unnötige weitere Risiken. Als DTS bietet wir Ihnen die Möglichkeit mit einer integrierten Sicherheitsplattform die Komplexität zu verringern und das Schutzniveau maximal zu erhöhen, mit den Zielen:

- Governance & Compliance in der Cloud
- Daten, Identitäten & Applikationen schützen (Identität als neuer Perimeter)
- Komplexität der Multi Cloud beherrschen
- DevOps-Security & DevSecOps-Prozesse

Die Bausteine für ene sichere Cloud-Umgebung

Unsere Bausteine für Ihre sichere Cloud sind:

- Next Gen Firewall (VM Series)
- Cloud Access Security Broker (CASB)
- Compliance & Workload Protection (Prisma Cloud)
- Authentifizierung (SAS)
- Device Identity as a Service (DIaaS)

Die virtuellen Firewalls der Palo Alto Networks VM-Series bieten umfassende Transparenz und Kontrolle über Umgebungen in der Multi Cloud und Hybrid Cloud. Sie lösen das Konzept mehrerer IT-Security Insellösungen ab. Sie können für Public Clouds wie Azure, AWS, GCP, softwaredefined Netzwerke und virtualisierte Umgebungen eingesetzt und von einem zentralen Management verwaltet werden. Somit dient es als wesentliches Sicherheitstool für konsistente Kontrolle in der Multi Cloud.

Die Möglichkeit die virtuellen Firewalls ebenfalls zur Segmentierung einzusetzen verkleinert die Angriffsfläche Ihrer Infrastruktur gegenüber Cyberangriffen. Das über alle Palo Alto Networks Firewalls einheitliche Security Featureset sorgt dafür, dass Bedrohungen erkannt und blockiert werden, bevor Schaden verursacht wird.

Der Wechsel in die Cloud kann Ihr Geschäft agiler, flexibler und effizienter machen. Gleichzeitig ist dieser Schritt mit verschiedenen Risiken in Bezug auf Datensicherheit und Compliance verbunden. Mit einem CASB lassen sich diese Risiken minimieren und die digitale Transformation absichern. Cloud-Sicherheit beginnt mit dem Schutz der Anwendungen, also SaaS-Applikationen wie Microsoft 365, Google G Suite, Salesforce, Box und andere. Es benötigt aber einen integrierten, personenorientierten Ansatz, der Bedrohungen korreliert und konsistente DLP-Richtlinien in E-Mail- und Cloud-Anwendungen durchsetzt. CASB schützt Sie vor Konten-Kompromittierung, versehentlicher Datenweitergabe, Konfigurationsfehlern in IaaS- und PaaS-Ressourcen und Compliance-Risiken. Unsere agentenlose Lösung bietet Ihnen personenorientierte Transparenz von Bedrohungen, eine anpassbare Zugriffssteuerung, automatisierte Reaktionen und umfassende Datensicherheit mit DLP.

Wenn Unternehmen ihre Entwicklungsprozesse modernisieren und auf cloudnative Architekturen umsteigen, stellen die Verantwortlichen schnell fest, dass ein auf Punktlösungen basierender Sicherheitsansatz nicht das Maß an Konsistenz und Kontrolle bietet, welches zur Sicherung der Cloud und der dort bereitgestellten Anwendungen, Daten und Infrastrukturen erforderlich ist. Prisma Cloud von Palo Alto Networks ist eine äußerst umfassende cloudnative Sicherheitsplattform, die Anwendungen, Daten und Cloud-bezogene Technologien mit einer branchenführenden Compliance und Workload

Protection während des gesamten Lifecycles in der Multi Cloud und Hybrid Cloud schützt. Die zentralen Funktionalitäten von Prisma Cloud umfassen:

- Management des Cloud-Sicherheitsniveaus (CSPM), also der komplette Überblick über alle implementierten Ressourcen und absolutes Vertrauen in deren Konfiguration und Compliance: Prisma Cloud nutzt einen eigenen Ansatz für das CSPM über das Compliance und Konfigurationsmanagement hinaus. Bedrohungsdaten aus über 30 Quellen liefern klare Informationen über akute Risiken und Sicherheitsmaßnahmen im Entwicklungsprozess sorgen dafür, dass unsichere Konfigurationen erst gar nicht in die Produktion gelangen.
    - Transparenz, Compliance & Governance
        - ein Verzeichnis der Cloud-Ressourcen
        - Konfigurationsprüfung in Echtzeit
        - Überwachung & Protokollierung der Compliance
        - Scans von Infrastructure-as-Code-Konfigurationen (IDE, SCM und CI/CD)
    - Bedrohungserkennung
        - Analyse des Anwender- & Objektverhaltens (UEBA)
        - API-basierte Netzwerkverkehrstransparenz, -analysen & -anomalieerkennung
        - automatisierte Untersuchung & Reaktion
    - Datensicherheit
    - Datenklassifizierung
    - Malware-Scans
    - Datengovernance
- Schutz von Cloud-Workloads, indem Prisma Cloud den gesamten Lebenszyklus, sowohl in der Public Cloud als auch in der Private Cloud sowie On-Premises schützt: problemlose Integration in die führenden CI/CD-Workflows, Registrys und Stacks
    - Hostsicherheit
        - Schwachstellenmanagement
        - Laufzeitschutz
        - Compliance-Management
        - Zugangskontrollen
        - Containersicherheit
        - Schwachstellenmanagement
        - Laufzeitschutz
        - Compliance-Management
        - Zugangskontrollen
        - Scannen von Git-Repositorys
    - Schutz serverloser Umgebungen
        - Schwachstellenmanagement
        - Laufzeitschutz
        - Compliance-Management
        - Zugangskontrollen

    - Sicherung von Webanwendungen & APIs
        - Schutz vor den OWASP Top-10
        - API-Schutz
- Netzwerksicherheit in der Cloud, also das konsistente Durchsetzen von Richtlinien: Prisma Cloud erkennt und verhindert Netzwerkanomalien, indem es Mikrosegmentierung auf Containerebene durchsetzt, Protokolldateien für den Datenverkehr untersucht und moderne, cloudnative Funktionen für die Bedrohungsabwehr auf Anwendungsebene (Layer 7) nutzt
    - Netzwerktransparenz & Erkennung von Anomalien
    - auf der Identität basierende Mikrosegmentierung
    - cloudnative Firewalls
- Management der Infrastruktur-Zugriffsrechte in der Cloud: Prisma Cloud durchsucht Umgebungen der IaaS und PaaS kontinuierlich nach Risiken für das Identitäts- und Zugriffsmanagement (IAM) und behebt diese automatisch
    - findet sämtliche Benutzer- & Maschinenidentitäten in allen Cloud-Umgebungen und analysiert deren Rechte, Rollen und Richtlinien
    - Überblick über Zugriffsrechte
    - IAM-Governance
    - automatisierte Reaktion
    - Analyse des Anwender- & Objektverhaltens (UEBA)

Mit der Cloud werden Verfahren zur Multi-Faktor-Authentifizierung (MFA) wichtiger, denn wenn Unternehmen ihre Systeme zunehmend in die Cloud auslagern und Benutzer nicht mehr zwingend dasselbe physische Unternehmensnetzwerk zum Zugriff auf Anwendungen und Daten nutzen, fällt dieser Sicherheitsfaktor weg. Als Ersatz müssen andere Sicherheitsmaßnahmen her, damit nur befugte Benutzer auf vertrauliche Ressourcen zugreifen können. Da die Cloud unterschiedlichen Benutzern jederzeit und von überall aus zur Verfügung steht, können mittels MFA zusätzliche Identitätsnachweise abgefragt werden, die sich nur schwer fälschen oder per Brute-Force-Angriff knacken lassen. So kann geprüft werden, ob ein Benutzer derjenige ist, für den er sich ausgibt. Mit dem DTS SafeNet Authentication Service (SAS) bieten wir Ihnen eine Zwei-Faktor-Authentisierung mit einer breiten Auswahl von Authentifizierungsoptionen an, welche einfach und universell für eine breite Anzahl an Applikationen und Geräte verfügbar ist. Durch die Bereitstellung eines Self Service Portals für Endanwender und den Betrieb der Plattform durch DTS profitieren Sie nicht nur von einer wesentlich erhöhten Sicherheit, sondern ebenso von deutlich verringertem Betriebsaufwand.

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de