AKAMAI-LÖSUNGSÜBERBLICK

Deloitte stärkt seine Angebote zur Vorfallsreaktion und Ransomware-Abwehr mit Akamai Guardicore Segmentation

Herausforderungen für den Kunden

Etablierte Sicherheitsproduktkategorien versprechen ein erhöhtes Schutzniveau vor den neuesten Bedrohungen für Unternehmensnetzwerke. Allerdings waren nur wenige Lösungen tatsächlich in der Lage, mit einer einzigen umfassenden Lösung die Angriffsfläche zu verringern – und zwar durch den Schutz vor schädlicher lateraler Netzwerkbewegung, egal, ob die Bewegung zu oder von der Hardware vor Ort, in der Cloud gehosteten Workloads, Endnutzergeräten oder Containern stattfindet. Darüber hinaus haben die ersten Zero-Trust-Segmentierungsinitiativen in der Vergangenheit Monate, wenn nicht gar Jahre in Anspruch genommen. Dies lag zum einen an technologischen Einschränkungen, jedoch auch an mangelndem Fachwissen in Bezug auf Angriffe, die gestoppt werden müssen, nachdem sie etablierte Sicherheitsprodukte wie veraltete Firewalls, EDR-Systeme und mehr bereits umgangen haben.

Bei Segmentierungsprojekten stehen Unternehmenskunden in der Regel vor den folgenden Herausforderungen:

- Fehlende Transparenz bei Assets, Netzwerkflüssen, Nutzern und Verbindungen in allen Umgebungen
- Begrenzte Sicherheitskontrollen für unterschiedliche Technologien und Infrastrukturen wie Hybrid-Cloud-Infrastruktur, ältere Betriebssysteme und OT/IoT
- Notwendigkeit zur Gewährleistung der Geschäftskontinuität, die häufig durch herkömmliche Segmentierungstechniken unterbrochen werden kann
- Mangel an Sicherheitsressourcen und -experten, um Initiativen zur Unterstützung von Zero Trust zu entwickeln, bereitzustellen und zu verwalten

Highlights der Lösung

Akamai Guardicore Segmentation ist die hostbasierte Mikrosegmentierungslösung, welche die einfachste, schnellste und intuitivste Methode zur Durchsetzung von Zero-Trust-Prinzipien im Netzwerk bietet. Akamai Guardicore Segmentation ist mit einer Mischung aus agentenbasierten Sensoren, netzwerkbasierten Datenkollektoren und Flussprotokollen von virtuellen Private Clouds zum Abbilden Ihres Netzwerks dafür konzipiert, eine einheitliche Visualisierung all Ihrer Assets und der gesamten Infrastruktur bereitzustellen (einschließlich älterer und moderner Betriebssysteme, Betriebstechnologie und IoT-Geräte). Damit können Sie ganz einfach Richtlinien erstellen und durchsetzen, die unerwünschte Kommunikation einschränken. So verringert sich Ihre Angriffsfläche und Sie stellen die Geschäftskontinuität sicher.

Wichtige Anwendungsfälle

- **Kontrolle im Bereich East-West-Traffic**
  Trennen Sie Umgebungen, Anwendungen, Nutzer und Infrastrukturen, die nicht miteinander kommunizieren müssen.
- **Abwehr von Ransomware**
  Implementieren Sie Richtlinienvorlagen mit KI/ML, um Angriffspfade zu blockieren, die bekanntermaßen von verschiedenen Arten von Ransomware-Angriffen verwendet werden.
- **Ringfencing von Anwendungen**
  Konzentrieren Sie sich auf die spezifischen Abhängigkeiten Ihrer geschäftskritischen Anwendungen, um strenge Sicherheitskontrollen erstellen zu können.

- **Nutzerbasierte Segmentierung**
  Verhindern Sie, dass Nutzer auf Anwendungen, Umgebungen und Geräte zugreifen können, die für ihre Arbeit nicht erforderlich sind.
- **Isolierung infizierter Geräte**
  Stoppen Sie die Ausbreitung eines Angriffs, wenn ein oder mehrere Geräte betroffen sind.
- **Compliance**
  Wenn Sie Ihr Netzwerk, Ihre Geräte und potenzielle Angriffswege kontextbezogen verstehen, sind Sie jederzeit in der Lage, Ihre Compliance unter Beweis zu stellen.

Vorteile für den Kunden

- Herausforderungen bei der Transparenz können mit einer einzigen Anzeige für das gesamte Netzwerk und alle Verbindungen, einschließlich Servern, Endpoints, Clouds, Containern, Nutzern und mehr gelöst werden.
- Zero-Trust-Richtlinien mindern die Möglichkeit eines erfolgreichen Ransomware-Angriffs.
- Die Reaktionszeit bei Vorfällen kann mithilfe von Bedrohungsinformationen und umfassenden Funktionen zur Angriffserkennung und -täuschung reduziert werden.
- Netzwerkforensik- und Compliance-Projekte werden mithilfe von Echtzeit- und Verlaufsfunktionen vereinfacht.

Die Expertise von Deloitte

1. **Beratung**
   Dank der Erfahrung von Deloitte mit effektiver Unterstützung bei Cybersicherheitsentscheidungen, Sicherheitslückenanalysen und der Erstellung von Implementierungs-Roadmaps können Unternehmenskunden stets fundierte Entscheidungen treffen – sowohl bei einem Angriff als auch, wenn sie für die Zukunft planen.
2. **Professional Services**
   Nutzen Sie vollständig verwaltete Implementierungsservices und profitieren Sie von nutzerdefinierten Integrationen in Ihre vorhandenen Sicherheits-, ITSM- und Cloudlösungen.
3. **Managed Services zur Vorfallsreaktion**
   Holen Sie sich im Falle eines Angriffs sofortige Unterstützung von den Deloitte-Experten, um diesen einzudämmen und weitere Angriffe in Zukunft zu verhindern.
4. **Lizenzabonnements**
   Deloitte bietet eine breite Palette von Lizenzabonnements an.

Kundenfallstudie: So lösen Akamai und Deloitte die Ransomware-Herausforderungen ihrer Kunden

Große Ransomware-Vorfälle haben dazu geführt, dass Kunden Beratung und Lösungen suchen, die zu einem kritischen Zeitpunkt sofort helfen können. Die Kombination der Fähigkeiten der Vorfallsreaktions- und Sicherheitsteams von Deloitte mit der Netzwerktransparenz, Angriffsforensik und Maßnahmen zur Reduzierung der Angriffsfläche von Akamai Guardicore Segmentation bieten genau das, was diese Kunden aktuell brauchen.

Hintergrund

Ein Unternehmen war von einem erheblichen Ransomware-Angriff betroffen, der das Kerngeschäft zum Erliegen brachte. Der Kunde wusste nicht, wo er ansetzen sollte, um das Problem zu lösen. Das gesamte Rechenzentrum, bestehend aus Tausenden von Servern, wurde gekapert und der Angriff musste umgehend auf sichere Weise eingedämmt werden. Wissend um unsere Expertise, wandte sich der Kunde sofort an Deloitte und wollte wissen, wie er vorgehen sollte. Das Deloitte-Team, das auf solche Situationen vorbereitet ist, konnte dem Kunden schnell ein Angebot zu Akamai Guardicore Segmentation machen und die Lösung bereitstellen. So konnte der Kunde schnell einen Überblick über das Ausmaß des Angriffs erlangen, nachvollziehen, welche Assets und Anwendungen betroffen waren, und alle zugehörigen Anwendungsabhängigkeiten identifizieren.

Lösung

Durch die Zuordnung der gesamten Kundenumgebung auf individueller Prozessebene konnte Akamai Guardicore Segmentation alle potenziellen Routen der Malware aus der kompromittierten Infrastruktur aufdecken. Dies ermöglichte es dem Deloitte-Team, sich für zusätzliche forensische Analysen nur auf bestimmte Teile des Netzwerks konzentrieren zu müssen. So wurde sichergestellt, dass nach der Wiederherstellung des Geschäftsbetriebs und des Zugriffs auf das Rechenzentrum keine Geräte mehr gefährdet waren.

Ergebnis

Nachdem der Ransomware-Angriff abgewehrt, das Rechenzentrum wieder in Betrieb genommen und der Geschäftsbetrieb wieder aufgenommen werden konnten, wurden sofort Maßnahmen ergriffen, um die Wahrscheinlichkeit eines erneuten Angriffs zu reduzieren. Wie viele Unternehmenskunden verwendet auch dieser Kunde einen mehrschichtigen Sicherheitsansatz mit mehreren führenden Lösungen zum Schutz von Geräten, Anwendungen, Nutzern und mehr. Da jedoch etwas so Einfaches wie eine Phishing-E-Mail einem Angreifer Zugriff gewähren kann, reichten diese Lösungen nicht aus, um den Angriff zu stoppen. Mit vollständiger Transparenz über das Netzwerk, die Anwendungsabhängigkeiten und die Nutzer, die Zugriff auf das Rechenzentrum haben, konnte der Kunde präzise Mikrosegmentierungskontrollen implementieren, um die Wege, die ein neuerlicher Ransomware-Angriff nutzen könnte, erheblich einzuschränken.

Nachdem der Kunde sich persönlich vom Wert der Lösung und der Expertise von Deloitte überzeugen konnte, beschloss er, auch in Zukunft auf diese zu vertrauen, um weiterhin von der Zero-Trust-Segmentierung zu profitieren. Außerdem beauftragte er Deloitte damit, sich um die tägliche Verwaltung der Lösung zu kümmern.

Fazit

Das umfassende technische Fachwissen und die Erfahrung mit Zero-Trust-Projekten macht Deloitte für Kunden zu einem idealen Partner für die Bereitstellung und Verwaltung von Akamai Guardicore Segmentation. Kunden können sich darauf verlassen, dass Deloitte diese Technologie für jede Sicherheitsinitiative verwendet, die eine Reduzierung der Angriffsfläche, die Kontrolle lateraler Netzwerkbewegungen, Ringfencing oder die Ransomware-Abwehr umfasst.

Über Deloitte

Deloitte bietet branchenweit unübertroffene Audit-, Steuer- und Beratungsdienste für viele der bekanntesten Marken weltweit, darunter fast 90 % der Fortune 500®-Unternehmen und mehr als 7.000 Privatunternehmen. Unsere Mitarbeiter setzen sich für Sie ein und arbeiten in allen Branchen, die den Markt von heute voranbringen und prägen. Wir liefern messbare und nachhaltige Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in unsere Kapitalmärkte zu stärken, Kunden zu inspirieren, Herausforderungen als Chancen für Wandel und Wachstum zu sehen und den Weg zu einer stärkeren Wirtschaft und einer gesünderen Gesellschaft zu ebnen. Deloitte ist stolz darauf, Teil des größten globalen Netzwerks für Professional Services zu sein, das unsere Kunden in den Märkten unterstützt, die für sie am wichtigsten sind. Unser Netzwerk von Mitgliedsunternehmen baut auf dem 175-jährigen Bestehen unseres Unternehmens auf und erstreckt sich über 150 Länder und Regionen. Erfahren Sie auf deloitte.com, wie sich die rund 415.000 Mitarbeiter von Deloitte weltweit vernetzen, um für Sie da zu sein.

Kontakt

Ola Sergatchov
Head of Global Strategic Alliances, Akamai
osergatc@akamai.com