SNAP SHOT

ENTSORGUNG + RECYCLING ZÜRICH
Progressive Stadt in der Schweiz verbessert Sicherheit mit Hilfe von Palo Alto Networks.

paloalto NETWORKS®

Version 1.4

SNAPSHOT

ENTSORGUNG + RECYCLING ZÜRICH

Progressive Stadt in der Schweiz verbessert Sicherheit mit Hilfe von Palo Alto Networks.

Stadt Zürich
Entsorgung + Recycling

Entsorgung + Recycling Zürich (ERZ) verwertet Abfälle aus der Stadt Zürich und führt wiederverwertbare Stoffe dem Recycling zu. ERZ sammelt täglich über 30.000 Abfallsäcke, reinigt die Strassen, Gehsteige und Parks und reinigt das Abwasser der Stadt Zürich. Mit etwa 900 Mitarbeitern ist ERZ die grösste Dienstabteilung im Tiefbau- und Entsorgungsdepartement von Zürich.

BRANCHE // Müllentsorgung, Recycling, Abwasserreinigung

HERAUSFORDERUNG // Verbesserung der Sicherheit zur Vermeidung fortgeschrittener Angriffe auf Endpoints, Reduzierung des IT-Verwaltungsaufwands und niedrigere CPU-Belastung.

LÖSUNG // Traps Advanced Endpoint Protection und WildFire wurden zur Enterprise Security-Plattform von Palo Alto Networks hinzugefügt.

ABONNEMENTS // Traps Erweiterte Endpoint Protection und Wildfire

HARDWARE // PA-4020

PA-4020 (1)

ERGEBNISSE

- Geringere Verwaltungskosten durch eine verlässlichere, automatisierte und einfach zu bedienende Endpoint-Security Lösung
- Verbesserte Visibilität der Sicherheitsvorfälle
- Durch die enge Integration der Palo Alto Security-Plattformen wurde ein neuer Level von Schutzmassnahmen geschaffen

Keine Zeitverschwendung

ERZ bietet der Bevölkerung von Zürich rund um die Uhr wichtige Infrastrukturdienste und erkennt deshalb, wie entscheidend es ist, sein Netzwerk zu schützen. Aufgrund der sich wandelnden Bedrohungen und der Einschränkungen seiner vorhandenen Endpoint-Security-Produkte suchte ERZ nach einer neuen Lösung. „Es traten Risiken wie Advanced Persistent Threats und andere auf", sagte Julio Lorenzo, Leiter Gruppe Fachinfrastruktur bei ERZ. „Unsere alten Virenschutzlösungen waren nicht in der Lage, uns vor diesen komplexen Angriffen zu schützen. Wir hatten keine verlässliche Endpoint Security. Wir benötigten mehr als nur Schutz am Internet-Gateway, um externe und interne Bedrohungen abzuwehren."

ERZ verwendet seit mehreren Jahren die Palo Alto Networks PA-4020 Next-Generation-Firewall für den Schutz des Netzwerks, Anwendungs- und Bandbreitenkontrolle und IPS. „Sie ist stabil, zuverlässig, leistungsfähig und bietet hervorragendes IPS und echte Anwendungskontrolle", sagte Lorenzo. „Palo Alto Networks bietet aber nicht nur Punkt-zu-Punkt-Sicherheit, sondern auch Sicherheit in der Anwendungsschicht."

Für den Virenschutz und den Schutz von Endpoints hatte ERZ im Laufe der Jahre mehrere Produkte von McAfee, Symantec, Hewlett-Packard und kürzlich von Kaspersky verwendet. Kaspersky erforderte vom verantwortlichen IT-Team mit 3 Personen übermässigen Verwaltungsaufwand und machte ERZ zusätzlich verwundbar. „Es war eine ständige Herausforderung, Sicherheitspatches rechtzeitig zu implementieren, um auf neue Schwachstellen oder Zero-Day-Angriffe zu reagieren", sagte Lorenzo. ERZ wollte eine moderne Endpoint-Security-Lösung, die keine zusätzlichen Ressourcen erforderte. "Wir suchen immer nach neuen Lösungen, durch welche die Arbeit und Threat Prevention automatisiert werden können. In der Vergangenheit bescherte uns dies einen Arbeitsaufwand von vier Stunden täglich", meinte Lorenzo.

Neudefinition der Endpoint Security

Omicron AG ist ein Anbieter von Sicherheitslösungen für zahlreiche Organisationen in der Schweiz und langjähriger IT-Berater von ERZ. Omicron AG empfahl Traps™ Advanced Endpoint Protection von Palo Alto Networks. Traps ist Teil der Enterprise Security-Plattform von Palo Alto Networks, die auch eine Next-Generation Firewall und Threat Intelligence Cloud enthält. Die

ENTSORGUNG + RECYCLING ZÜRICH

Progressive Stadt in der Schweiz verbessert Sicherheit mit Hilfe von Palo Alto Networks.

Enterprise Security-Plattform bietet Transparenz und Kontrolle für Anwendungen, Benutzer und Inhalte. Zudem schützt sie vor bekannten und unbekannten Cyberbedrohungen. Die Threat Intelligence Cloud bietet eine zentrale Daten Informationsfunktionalität.

Traps verhindert komplexe Exploits von Schwachstellen und durch unbekannte Malware durchgeführte Angriffe. Es ist ein extrem skalierbarer, leichter Agent und verwendet eine innovative Methode zur Verhinderung von Angriffen, ohne, dass die Bedrohung vorher bekannt gewesen sein musste. Traps bietet Organisationen ein leistungsfähiges Werkzeug zum Schutz von Endpoints vor praktisch jedem gezielten Angriff.

ERZ testete Traps in seinem Labor. „Wir mussten nicht einmal den Test eines anderen Endpoint-Security-Produkts in Erwägung ziehen", sagte Lorenzo. „Traps bietet einen extrem zuverlässigen, starken Schutz im Lebenszyklus von Cyberangriffen – viel besser als Legacy-Virenschutzlösungen. Zudem hat es eine andere, auf Prävention ausgelegte Methode der Endpoint Security." Ein weiteres wichtiges Argument war die Benutzerfreundlichkeit. „Wir müssen Traps nicht dauernd im Auge behalten und aktualisieren, und dennoch kann es unbekannte Angriffe verhindern", so Lorenzo.

Keine wiederverwerteten Lösungen

ERZ ersetzte Kaspersky durch Traps. „Patches sind nicht mehr zeitraubend oder dringend, da Traps uns selbst vor der Implementierung der Patches schützt", sagte Lorenzo. „Traps erfordert auch nur geringe Verwaltungsarbeit und absorbiert keine Ressourcen. Vorher liefen unsere Lösungen andauernd und verbrauchten unnötigerweise Ressourcen. Traps wird nur aktiv, wenn es gebraucht wird."

Lorenzo ist von der Skalierbarkeit und dem geringen Ressourcenverbrauch von Traps begeistert. „Es wirkt sich überhaupt nicht auf die Leistung aus", meinte Lorenzo. „Man kann Traps an verschiedenen Stellen einsetzen und leicht unterschiedliche Netzwerke abdecken. Zudem kann man es mit nur minimaler Schulung benutzen."

Als ERZ Traps einführte, abonnierte es auch Palo Alto Networks WildFire™. Ein Abonnement von WildFire schützt gegen fortgeschrittene Malware und Bedrohungen, indem es unbekannte Malware, Zero-Day-Exploits und Advanced Persistent Threats (APTs) proaktiv identifiziert und blockiert. WildFire erweitert die Enterprise Security-Plattform von Palo Alto Networks und wendet seine Verhaltensanalyse auf einzigartige Weise unabhängig von Port oder Verschlüsselung an. Wenn eine unbekannte Bedrohung entdeckt wird, sorgt WildFire automatisch für Schutz und blockiert die Bedrohung beinahe in Echtzeit über den Lebenszyklus von Cyberangriffen hinweg.

„WildFire bietet eine weitere Ebene des Schutzes", sagte Lorenzo. „Die direkte Integration zwischen Traps und WildFire bedeutet, dass unbekannte ausführbare Dateien, die versuchen, auf Endpoints zu laufen, automatisch überprüft werden. Wenn die Datei schädlich ist, wird Traps die Ausführung verhindern. Zudem kann selbst unbekannte Malware aufgehalten werden, da Traps unbekannte ausführbare Dateien zur Analyse an WildFire sendet."

Fortschrittliche schweizerische Abteilung erhält fortschrittliche Sicherheit

ERZ ist froh, dass es seine Sicherheit Palo Alto Networks anvertraut hat. "Mir gefällt die Einfachheit von Traps, dass es eine im Vergleich zu den typischen Virenschutzprodukten innovative, völlig neue Methode verwendet, und dass es weniger Ressourcen erfordert", meinte Lorenzo. "Die hauptsächlichen Einsparungen betreffen Personalaufwendungen. Administrative Kosten konnten gegenüber den nicht mehr funktionierenden AV Lösungen erheblich gesenkt werden".

ERZ hat die Endpoint Security und die allgemeine Sicherheit verbessert und den IT-Verwaltungsaufwand reduziert. „Es gibt keine Wunderwaffe in der IT-Sicherheit", meinte Lorenzo. „Vom Schutz des Netzwerkrands bis zum Endpunkt muss alles präzise integriert sein, da man nie weiss, woher Bedrohungen kommen können. Die in die Enterprise Security-Plattform von Palo Alto Networks integrierte Traps Endpoint Security zeigt einem, was passiert, wo es passiert, und sie stoppt Bedrohungen. Das bietet ein neues Niveau an Schutz und Prävention gegen bekannte und unbekannte Bedrohungen, bevor sie Schaden anrichten können."

paloalto NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

www.omicron.ch

Omicron AG
Thomas Stutz
Inhaber & Geschäftsleitung
Mail: thomas.stutz@omicron.ch
Phone: +41 44 839 11 11
Mobil: +41 79 839 11 11