APT PROTECT PRO (CLOUD)

ZERO-DAY-SCHUTZ

EINFÜHRUNG

Cyber-Kriminelle haben es heute leicht, Exploit-Code und neue Schwachstellen für gezielte Angriffe (Advanced Persistent Threats) zu verwenden. Anti-Virus, Next Generation Firewalls und andere zentrale Sicherheitslösungen beschränken sich ausschließlich auf bekannte Bedrohungen und herkömmliche Sandbox-Lösungen sind den heutigen Angriffen nicht mehr gewachsen. Neben hochentwickelten Penetrationsmethoden nutzen Angreifer immer mehr komplexe Methoden, um herkömmliche Sicherheitslösungen zu umgehen.

Um die modernsten unbekannten Zero-Day-Gefahren zu erkennen, sind daher neue gleichermaßen hochentwickelte Sicherheitsmethoden erforderlich. Telekom Security, der Vorreiter in Sachen Managed Security Services, bietet mit APT Protect Pro (Cloud) erneut die richtige Lösung. APT Protect Pro (Cloud) ist ein Security-as-a-Service zur sicheren Emulation von E-Mail-Anhängen, welches das branchenführende Sandboxing auf Betriebssystemebene durch einen Schutz auf CPU-Ebene ergänzt. Zusammen mit den Lösungen Threat Extraction und Zero-Day-Protection hält APT Protect Pro (Cloud) die betriebliche Agilität und Kontinuität aufrecht.

Mit APT Protect Pro (Cloud) werden eine Vielzahl von Dateiformaten einschließlich Exe- und Datendateien auf Betriebssystem- und CPU-Ebene überprüft. Dafür kommen eine umgehungssichere Malware-Erkennung und umfassender Schutz vor den gefährlichsten Angriffen zum Einsatz – gleichzeitig wird die schnelle Zustellung der sicheren Inhalte an Ihre Anwender gewährleistet. APT Protect Pro (Cloud) führt eine Tiefenprüfung auf CPU-Ebene aus, was auch die gefährlichsten Angriffe stoppt, bevor Malware die Möglichkeit hat, ihre Tätigkeit aufzunehmen und einer Erkennung zu entgehen. D.h. die Engine der Lösung prüft den CPU-basierten Befehls-Fluss auf Exploits, die Sicherheitsmaßnahmen auf Hardware- und Betriebssystemebene umgehen sollen. Mit dieser einzigartigen Prüfungsmethode liefert APT Protect Pro (Cloud) bestmögliche Erkennungsrate für Bedrohungen und ist praktisch immun gegen die Umgehungstechniken der Angreifer.

Ergänzt wird diese Lösung durch die sofortige Bereitstellung sicheren Contents oder sauberer und wiederhergestellter Versionen potenziell schadhafter Dateien. Damit eliminiert APT Protect Pro (Cloud) die inakzeptablen Verzögerungen herkömmlicher Sandboxing-Syteme und ermöglicht einen Real-World-Einsatz im Vermeidungsmodus.

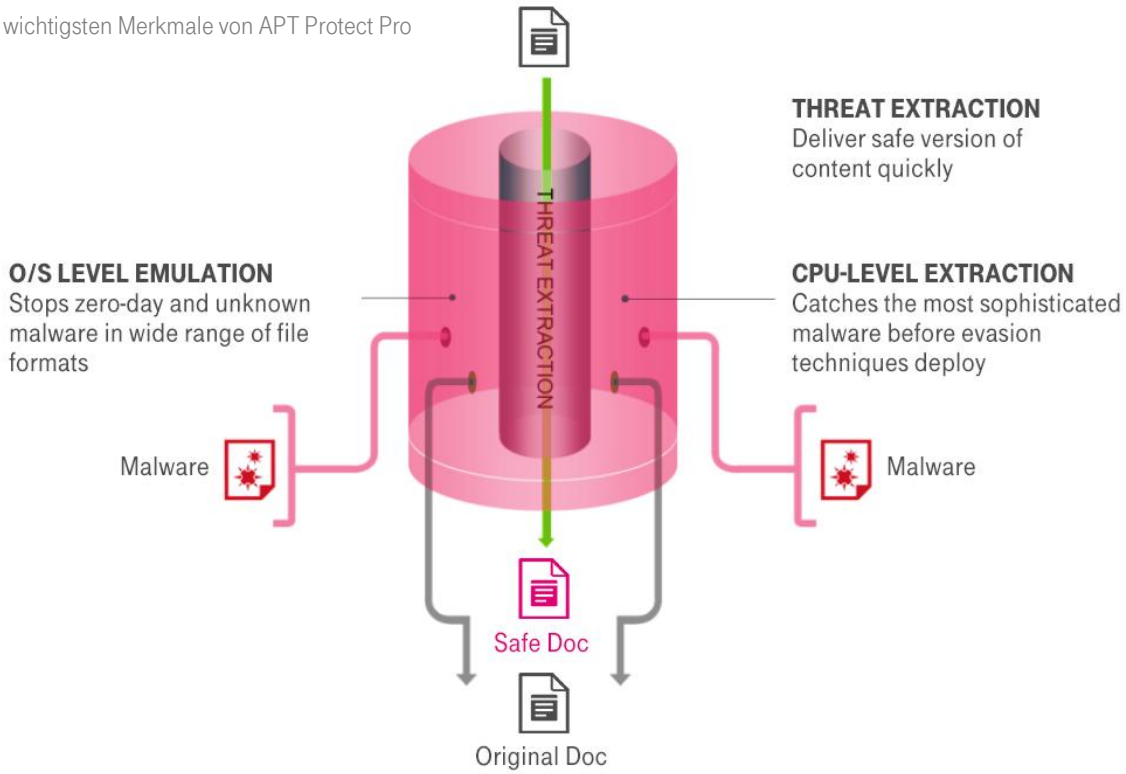
DIE VORTEILE IM ÜBERBLICK

- Security-as-a-Service zum Schutz von Mail-Verkehr vor gezielte Angriffen (Advanced Persistent Threats)
- Keine Installation von Hardware oder Software erforderlich
- Beste Erkennungsrate von unbekannter Malware
- Identifiziert und blockiert Gefahren schon in ihren Anfängen
- Schnelle Wiederherstellung von Dateien und Bereitstellung sicherer Inhalte
- Reduziert das Risiko teurer Datendiebstähle oder Betriebsunterbrechungen
- Der integrierte Schutz maximiert den betriebswirtschaftlichen Wert und reduziert die Gesamtbetriebskosten (TOC)

DIE FUNKTIONEN IM ÜBERBLICK

- Gründliche Prüfung von Malware auf CPU-Ebene, wo sich Exploits nicht verbergen können
- Sicherer Schutz für eine Vielzahl von Dokument- und Dateiformaten
- Funktioniert mit vorhandener Infrastruktur; keine Installation neuer Ressourcen erforderlich
- Entfernt aktive und sonstige ausnutzbare Inhalte aus Dokumenten
- Automatische Aktualisierung von Bedrohungsinformationen

Bild 1: Die wichtigsten Merkmale von APT Protect Pro



LIFE IS FOR SHARING.

LÖSUNGSARCHITEKTUR

EINSATZMÖGLICHKEITEN

APT Protect Pro (Cloud) kann auf zwei verschiedene Arten in die vorhandene Infrastruktur integriert werden.

Bei der ersten Option wird die Lösung als Zusatzfunktion zu E-Mail Protect Pro eingesetzt. E-Mail Protect Pro ist ein Cloud-basierter SaaS-Angebote der Telekom Security, der Schutz vor Spam und Viren bieten. In diesem Fall weist der MX-Eintrag direkt auf E-Mail Protect Pro und die Lösung leitet (auf Basis TLS) Mails an APT Protect Pro (Cloud) weiter.

Bild 2: Erste Einsatzmöglichkeit – Kombination mit Business Mail Protect bzw. Managed Anti Spam

Bei der zweiten Option zeigt der MX-Eintrag weiterhin auf die derzeit genutzte Third Party Antivirus/Antispam-Lösung. In diesem Fall ist der nächste Hop APT Protect Pro (Cloud). Nach der Emulation wird die Mail an den Nutzer gesendet. Diese Art der Integration ist ausschließlich für bestimmte Third Party Lösungen möglich.

Bild 3: Zweite Einsatzmöglichkeit - Kombination mit Third Party Antivirus/Antispam

Auch Kunden mit Office 365 können APT Protect Pro nutzen, indem der MX-Eintrag mit Ziel auf E-Mail Protect Pro geändert wird. APT Protect Pro bietet damit Zero-Day-Schutz auch für Ihre Geschäftsanwendungen in der Cloud.

DIE UNTERSCHIEDLICHEN PROFILE

APT Protect Pro (Cloud) stoppt Angriffe, bevor sie im Unternehmen ihre Wirkung entfalten können. Die Kombination aus Emulation auf Betriebssystem und CPU-Eeben führt zu einem deutlich höheren Schutz ohne zusätzliche Latenzen. Um ein durchgängig hohes Sicherheitsniveau und Einfachheit sicherzustellen, können Kunden aus drei verschiedenen Profilen auswählen. Auf Kundenwunsch kann während der Vertragslaufzeit das Profil (Detect/ Prevent/Prevent Plus) über den 24/7-Support geändert werden.

DETECT	PREVENT	PREVENT PLUS / EXTRACT
▪ Dateien werden zugestellt und parallel emuliert. ▪ Reines Reporting. ▪ Ziel: Nachvollziehen an welcher Stelle Malware bzw. malicious Content gefunden wurde.	▪ Mails einschließlich Dateien werden in APT Protect Pro zwischengespeichert und parallel emuliert. ▪ Nach erfolgreicher Emulation wird die Mail an den Nutzer gesendet ▪ Wenn Malware erkannt wird, wird der Anhang entfernt und der Nutzer informiert.	▪ Eliminierung von Dokumenten-Bedrohungen in Echtzeit durch Entfernen von aktiven Inhalten (z.B. Makros) oder eingebetteten Links. ▪ Nutzer erhalten immer E-Mails mit sicheren Dokumenten. ▪ Zugriff auf die Original-Datei möglich: Der Nutzer klickt auf einen Link, den APT Protect Pro an die E-Mail anhängt. Die Emulation wird angestoßen und die Datei dem Nutzer zugestellt.



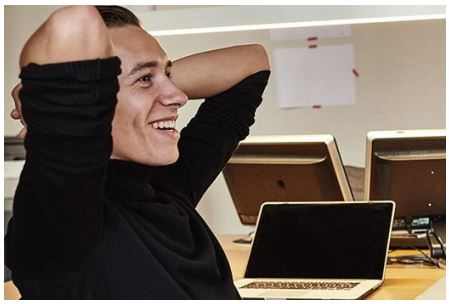


Bild 4: Profile von APT Protect Pro

RECHENZENTRUM

APT Protect Pro (Cloud) wird am neuen Rechenzentren Twinning-Standort Biere/Magdeburg gehostet. Es handelt sich hierbei um einen wichtigen Hub in der weltweiten Rechenzentrumsinfrastruktur des Managed Security Service Providers Telekom Security. Das Rechenzentrum ist der größte Cloud-Computing-Standort Deutschlands und einer der größten in ganz Europa. Aktuell ist eine Fläche von 5400 qm belegt. Die Rechenrenztren umfassen rund 30.000 Server welche auf einer Fläche von fast 40.000 qm verteilt sind. Mit dem neuen Standort will die Telekom der rasant wachsenden Nachfrage nach Cloud-Diensten in Deutschland und Europa begegnen. Die Gebäudekomplexe sind vollständig abgeschirmt. Höchste Sicherheitsvorkehrungen schützen die Daten vor unberechtigtem Zugriff. Durch Kombination von Hochleistungsrechenzentren mit schnellen sicheren Netzwerken bietet die Telekom eine Plattform für fortschrittliche Technologien wie Industrie 4.0, IoT, Security-as-a-Service und Big Data-Analysen.