CLOUD OFFICE SECURITY

VERFÜGBAR ALS MANAGED SERVICE

SITUATION

Ein schnell wachsendes Unternehmen arbeitet mit verschiedenen Microsoft 365 Cloud-Anwendungen wie bspw. Exchange Online, Microsoft Teams, SharePoint und OneDrive. Dabei hat es immer wieder mit Spam-Mails, Phishing-Attacken und schadhaften Dateianhängen zu kämpfen. Durch den Zuwachs an Personal ist das IT-Team zudem stark mit dem Rollout von Nutzer- und Gruppenrechten ausgelastet. Der IT-Verantwortliche sucht daher am Markt nach geeigneten Lösungen, um gegen die Bedrohungen vorzugehen und die Rollout-Prozesse zu automatisieren, damit die IT-Abteilung dem Tagesgeschäft wieder nachgehen kann.

UND JETZT?

Die Organisation ist in diverse Abteilungen aufgegliedert, für die verschiedene Sicherheitseinstellungen vorgesehen sind. Alle neuen Mitarbeiter sollen benötigte Rechte und optimalen Schutz umgehend mittels automatischen Rollouts erhalten. Die Nutzer sollen bei ihrer täglichen Arbeit mit den cloudbasierten Tools umfassend und automatisch jederzeit geschützt sein. Der Arbeitsaufwand ist dabei für die IT-Abteilung so gering wie möglich zu halten und die Sicherheitslösung sollte Funktionen zur Unterstützung bei auftretenden Bedrohungen bereitstellen.

ESET HAT DIE LÖSUNG

3 GRÜNDE FÜR ESET CLOUD OFFICE SECURITY

HÖHERES SCHUTZNIVEAU

ESET Cloud Office Security bietet umfassenden und präventiven Schutz von Microsoft 365 Cloud-Anwendungen inkl. cloudbasierter Sandbox-Analyse zur Erkennung neuer sowie unbekannter Bedrohungen. Damit werden bestehende Bordmittel um Multi-Vendor-Strategien im Rahmen der Compliance-Anforderungen wirkungsvoll ergänzt.

VOLLAUTOMATISIERTES ROLLOUT

Neue Nutzer und Gruppen einer Microsoft 365 Umgebung sind auf Wunsch automatisch geschützt und müssen nicht separat über die Web-Konsole hinzugefügt werden. Der Admin erhält bei Gefahrenerkennung Benachrichtigungs-E-Mails und kann bei Bedarf sofort reagieren.

QUARANTÄNE

Verdächtig eingestuften E-Mails, Anhänge und Dateien werden in separatem Bereich des Cloud-Speichers aufgelistet. Dort kann vom Administrator entschieden werden, ob entsprechende Elemente eliminiert oder für das Netzwerk freigegeben werden.

DIE WICHTIGSTEN EIGENSCHAFTEN IN KÜRZE:

- Filtert Spam-E-Mails, bereinigt Postfächer von unangemessenen Inhalten und ermöglicht Black-/Whitelisting für Exchange Online zu konfigurieren
- E-Mail-Inhalte werden auf Phishing-Links (URLs) geprüft, abgeglichen und bei Verdacht sofort blockiert
- Scannen von E-Mails, Anhängen sowie Dateien in OneDrive, SharePoint oder Microsoft Teams zum präventiven Schutz vor Malware
- Bietet eine breite Auswahl an Protokollen und Filtern zur Nachverfolgung von Meldungen sowie ein zugängliches Berichtswesen
- Multimandantenfähigkeit für MSP-Administratoren
- Richtlinienbasierte Sicherheitseinstellungen, die ausgewählten Nutzern zugewiesen und an deren Bedürfnisse angepasst werden können