Bleiben Sie aktuellen hochentwickelten E-Mail-Angriffen einen Schritt voraus

Managed Service für Advanced Email Security

E-Mail ist der Bedrohungsvektor Nr. 1 bei Cyber-Angriffen

Alle Unternehmen stehen vor der gleichen großen Herausforderung: E-Mail ist für Unternehmen das wichtigste Kommunikationstool und gleichzeitig der häufigste Angriffsvektor für Kompromittierungen.

Schützen Sie Ihre Firmen-E-Mails vor aktuellen Bedrohungen

Cyberkriminelle nutzen E-Mails zu verschiedenen Zwecken – zur Übertragung von Malware auf ein Unternehmenssystem, zum Diebstahl von Daten oder um per Social Engineering Geld zu erbeuten. Sie benötigen daher Schutzmaßnahmen, die hochentwickelte Bedrohungen in eingehenden E-Mails schnell erkennen und blockieren können, um die Marke, den Ruf und die Daten Ihres Unternehmens zu schützen.

Was ist der Managed Service für Advanced Email Security?

Unser Managed Service für Advanced Email Security unterstützt Sie mit unserem ganzen Know-how und den effektivsten Technologien der nächsten Generation beim umfassenden Schutz Ihres Unternehmens vor einem breitem Spektrum an E-Mail-Bedrohungen.

Nachgewiesener Erfolg

Immer mehr Unternehmen entscheiden sich für unseren Managed Service für Advanced Email Security, um diese Bedrohungen abzuwehren:

Phishing- und BEC-Angriffe (Business Email Compromise)

Hacker nutzen Informationen aus sozialen Medien, um Mitarbeiter zur Weitergabe vertraulicher Informationen zu bewegen.

Kontoübernahmen

Cyberkriminelle übernehmen die Kontrolle über ein legitimes Konto und führen darüber böswillige Aktionen aus.

Zero-Day-Malware und hochentwickelte permanente Bedrohungen

Bei diesen Angriffen kommen kontinuierliche und hochentwickelte Hacking-Techniken zum Einsatz, die langfristigen Zugang zu einen System gewähren.

cybite that's IT!

Schon gewusst?

Phishing ist eine Form von Online-Betrug, bei dem ein Angreifer legitime Organisationen in E-Mails, Textnachrichten oder Werbung nachahmt, um ein Opfer zur Weitergabe vertraulicher Informationen an den Angreifer zu verleiten oder schädliche Software auf dem Gerät des Opfers zu verteilen.

90 %
der erfolgreichen Cyber-Angriffe werden durch E-Mails ausgelöst
↘ **Mehr erfahren**

4,24 Mio USD
weltweite Durchschnittskosten bei einer Datenkompromittierung im Jahr 2021
↘ **Mehr erfahren**

58 %
der Umfrageteilnehmer haben bis zu drei Arbeitsstunden durch Spam verloren
↘ **Mehr erfahren**

Vorteile

- Schutz vor gezielten Phishing-Angriffen und E-Mail-Betrugsversuchen
- Stoppen von Ransomware und Zero-Day-Malware, bevor sie das Postfach erreichen
- Schutz Ihres Teams vor Klicks auf schädliche Links für alle Geräte dank URL-Filterung
- Blockierung neuer Bedrohungen durch Echtzeit-Threat Intelligence
- Sofortige Produktivitätssteigerung durch Spam-Kontrolle
- Zuverlässige E-Mail-Zustellung ohne Beeinträchtigung der Produktivität
- Stoppen von Spoofing- und BEC-Versuchen gegen Ihr Unternehmen
- Verhinderung von Kontoübernahmen und Überwachung interner Postfächer auf Anzeichen von Kompromittierung

Die nächsten Schritte

Kontaktieren Sie uns, um mehr über unseren Managed Service für Advanced Email Security zu erfahren:

cybite GmbH & Co.KG business@cybite.de | +492921321010 https://www.cybite.de

Keine Produktivitätseinbußen durch Spam

Spam ist nicht nur lästig, sondern beeinträchtigt auch die Produktivität im Unternehmen und stört Ihre Mitarbeiter bei der Erledigung ihrer Aufgaben. Die Zeit, die durch das Löschen unnötiger E-Mails verschwendet wird, ist dabei das geringste Problem. Denn Spam kann auch schwerwiegende Schäden verursachen, zum Beispiel durch die Infektion der Mitarbeiterrechner mit Schadsoftware, die die Systeme beeinträchtigt und private oder geschäftliche Informationen stiehlt.

Schützen Sie Microsoft 365, Google Workspace oder andere Cloud-basierte bzw. lokale Postfächer vor hochentwickelten Bedrohungen

Kontoübernahmen

Kontoübernahmen bei Microsoft 365, Google Workspace oder Open-Xchange durch Anmeldedaten-Phishing zählen zu den drei häufigsten E-Mail-Bedrohungen. Wir schützen Sie nicht nur vor Phishing-Versuchen, die es auf die Anmeldedaten Ihrer Mitarbeiter abgesehen haben, sondern überwachen E-Mail-Konten zudem auf verdächtige Aktivitäten, die auf eine Kompromittierung hindeuten könnten. Sicherheitslücken in Ihren Postfächern werden somit schnell und zuverlässig geschlossen.

BEC

Bei BEC-Angriffen werden Personen im Unternehmen imitiert (z. B. Führungskräfte oder Geschäftsführer), um die Benutzer dazu zu bringen, betrügerische Überweisungen durchzuführen oder vertrauliche Informationen herauszugeben. Sie benötigen daher zusätzliche E-Mail-Schutzmaßnahmen, die auch hochentwickelte Angriffe ohne Schaddaten erkennen und stoppen können, bevor sie die Benutzer erreichen. Außerdem müssen Sie die potenziellen Auswirkungen von Kompromittierungen einschränken, ohne die alltägliche E-Mail-Kommunikation zu beeinträchtigen.

Microsoft 365 · Google Workspace · Exchange · OX

Und viele mehr ...

Schützen Sie Ihre Firmen-E-Mails vor allen Arten von Angriffen.