KASPERSKY SECURITY FOR MICROSOFT EXCHANGE SERVERS

Risikominderung beim Verlust vertraulicher Daten über Unternehmens-E-Mails

Eines der größten Sicherheitsprobleme im Bereich E-Mail stellt sich heutigen Sicherheitsexperten aus dem Grund, dass immer mehr wichtige Unternehmensdaten oder persönliche Daten verloren gehen. E-Mail-basierte Malware führt zur Unterbrechung des Betriebs und kostspieligen Ausfallzeiten, und Spam wirkt sich zunehmend negativ auf die Mitarbeiterproduktivität und die Serverressourcen aus, doch der Verlust vertraulicher Daten kann für die Finanzen und den Ruf eines Unternehmens einen nicht wieder gutzumachenden, langfristigen Schaden bedeuten.

Kaspersky Security for Microsoft Exchange Servers löst dieses Problem durch das Ermitteln vertraulicher Daten und deren Kontrolle bzw. Blockierung beim Übermitteln per E-Mail. Unterstützt werden diese Funktionen durch einen intelligenten und zuverlässigen Spam- und Malware-Schutz.

- Identifikation und Analyse vertraulicher Daten
- Flexible Kontrolle der Übermittlung per E-Mail
- Spam-Schutz in Echtzeit mit wenigen Fehlalarmen
- Phishing-Schutz
- Fortschrittlicher, Cloud-basierter Malware-Schutz
- Detaillierte Benachrichtigungen und Reporting
- Unkompliziertes, zentrales Management
- Getrennte Funktionen für Übermittlungskontrolle und Sicherheit

SCHUTZ VOR DATENVERLUST UND KONTROLLE

Durch Ermitteln von Geschäfts-, Finanz-, persönlichen und anderen vertraulichen Daten in ausgehenden E-Mails und Anhängen und die Kontrolle dieses Informationsflusses sorgt Kaspersky Security for Microsoft Exchange Servers dafür, dass Ihre vertraulichen Daten und die Ihrer Mitarbeiter stets geschützt sind und Sie die gesetzlichen Datenschutzauflagen erfüllen. Dank ausgeklügelter Analysetechniken wie die Suche nach strukturierten Daten und unternehmensspezifische Glossare können verdächtige E-Mails identifiziert und somit blockiert werden. Das System kann sogar den Vorgesetzten des Absenders per E-Mail auf eine potentielle Datensicherheitsverletzung aufmerksam machen.

INTELLIGENTE SPAM-ERKENNUNG UND -ANALYSE

Intelligente Technologien bieten optimale Erkennungsraten und blockieren Spam effektiv unter minimalem Auftreten von Fehlalarmen (False Positives). Analyse- und Blockier-Tools für den Phishing- und Spam-Schutz werden effektiv durch Cloud-basierte Bedrohungsmeldungen in Echtzeit unterstützt, wobei die flexible Kontrolle dafür sorgt, dass „Grauzonen“ unerwünschter E-Mails separat klassifiziert und verarbeitet werden.

ECHTZEITSCHUTZ VOR MALWARE

Nachrichten und Anhänge werden in Echtzeit gescannt, sodass alle Arten von Malware erkannt und entfernt werden. Unterstützt wird dies wiederum durch das Cloud-basierte Kaspersky Security Network, das selbst Exploits erkennt, die es auf Zero-Hour-Schwachstellen abgesehen haben. Da die gespeicherten Nachrichten im Hintergrundmodus gescannt werden, wird die Serverbelastung minimal gehalten.

FLEXIBLE VERWALTUNG

Eine zentrale Verwaltung mit umfassenden Konfigurationsfunktionen und einem flexiblen Reporting- und Meldungssystem ermöglichen dem Administrator, den Strom vertraulicher Daten über E-Mail zu kontrollieren sowie das IT-System vor Malware-Bedrohungen und Ressourcenverschwendung durch Spam zu schützen.

FUNKTIONEN

DATENSICHERHEIT

Ermitteln vertraulicher Daten: Die Lösung implementiert Module, die bestimmte Datentypen in E-Mails und Anhängen anhand individueller Kategorien wie persönliche Daten und Bankkartendaten erkennen. (Gleichzeitig wird sichergestellt, dass die gesetzlichen Datenschutzauflagen erfüllt werden.) Darüber hinaus führt das Programm Scans mithilfe vorinstallierter Themenglossare durch, z. B. „Finanzen“, „Verwaltungsdokumente“ und „Beleidigendes und obszönes Vokabular“, die regelmäßig aktualisiert werden.
Unternehmensspezifische Glossare: Es können Glossare mit unternehmensspezifischen und sogar projektspezifischen Schlüsselwörtern und Ausdrücken erstellt werden, um die meisten vertraulichen Geschäftsinformationen in ausgehenden E-Mails abzufangen. Glossare können auch über eine Abfragesprache erstellt werden.
Tiefgreifende Analyse anhand von strukturierten Daten: Als Suchobjekt können auch strukturierte Daten dienen. Eine Kombination bestimmter Datentypen innerhalb derselben Nachricht oder Daten in komplexen Arrays, wie sie beispielsweise in Kundendatenbanken vorhanden sind, können als vertrauliche Informationen identifiziert werden.

SPAM-SCHUTZ

Intelligente Spam-Erkennungstechnologien: Elemente wie die E-Mail- und IP-Adresse des Absenders, Nachrichtengröße und Titel sowie Inhalt und Bilder werden mithilfe von intelligenten Technologien analysiert, die einzigartige visuelle Signaturen zur Erkennung von visuellem Spam einsetzen. Die Reputationsfilterung wirkt unbekanntem Spam entgegen, indem verdächtige E-Mails isoliert und erneut analysiert werden. So lässt sich die Häufigkeit von Fehlalarmen weitgehend einschränken.
Cloud-basierter Echtzeitschutz: Dank der Integration mit dem Kaspersky Security Network (KSN) werden Reputationsfilterung und Anti-Phishing-Technologien durch Echtzeitinformationen zu neuen Spam-Bedrohungen unterstützt.
Nachrichtenklassifizierung: Unerwünschte Nachrichten können anhand von Kategorien verarbeitet werden, um zu gewährleisten, dass wichtige E-Mails nicht verloren gehen. Offensichtliche Spam-Nachrichten können blockiert und verdächtige Nachrichten an einen Ordner für unerwünschte E-Mails weitergeleitet werden, während Servicenachrichten (z. B. Zustellungs- und Empfangsbelege) an den Posteingang gesendet werden.

ANTI-MALWARE

Echtzeit-Scans des Datenverkehrs: Erkennt und löscht alle Arten von Viren, Würmern, Trojanern und anderer Malware in ein- und ausgehenden Nachrichten und Anhängen. Die Integration mit dem Kaspersky Security Network (KSN) ermöglicht Warnmeldungen zu neuen und potentiellen Malware-Bedrohungen in Echtzeit.
Hintergrund-Scans: Da die gespeicherten Dateien auf Abruf und gemäß Zeitplan im Hintergrund gescannt werden können, wird der Arbeitsaufwand für den Server so gering wie möglich gehalten.
Sicherungskopien: Sicherungskopien aller gelöschten Nachrichten werden zu Analyse- oder Wiederherstellungszwecken (im Fall eines Klassifizierungsfehlers) aufbewahrt.

Detaillierte Informationen erhalten Sie auf dieser Webseite: www.kaspersky.com/de/business-security/microsoft-exchange-server-antivirus

VERWALTUNG

Zentralisierte Verwaltung: Um die Sicherheit aller Microsoft Exchange-Server zu verwalten, wird eine einzige Verwaltungskonsole mit zentralen Reporting-Funktionen in die Managementkonsole von Microsoft integriert. Aktivitäten im Bereich Sicherheits- und Übermittlungsmanagement für vertrauliche Daten können bei Bedarf auch verschiedenen Personen mit unterschiedlichen Rollen zugewiesen werden.
Umfassende Konfigurationsfunktionen: Die Einhaltung der Sicherheitsrichtlinien des Unternehmens kann in Einklang mit den verfügbaren Ressourcen gebracht werden, indem beispielsweise bestimmte Dateitypen oder Nachrichtenkategorien aus den Scans ausgenommen oder bei Anti-Spam-Scans unterschiedliche Level auf verschiedene Kategorien angewendet werden. Es ist zudem möglich, Whitelists und Blacklists von Absender- und Empfängeradressen zu erstellen und anzuwenden.
Richtlinien zur Übermittlungskontrolle für Informationen: Sie können spezielle Richtlinien erstellen, um die Übermittlung vertraulicher Daten zu kontrollieren und die Reaktion auf Datenverlustvorfälle festzulegen, beispielsweise durch Blockieren oder Zulassen von Nachrichten und durch Festlegen von Risikolevels.

REPORTING

Flexibilität bei Reporting und Meldungen: Mithilfe der Verwaltungskonsole können Sicherheitsstatus und -aktivitäten, einschließlich der Übermittlung vertraulicher Informationen, überprüft werden. Inhalt und Häufigkeit der Berichte können angepasst werden. Das Management von Ereignismeldungen erfolgt über Microsoft Windows® Standard-Tools.
Analyse von Versuchen zur Übermittlung vertraulicher Daten: Anhand detaillierter Informationen zu allen Vorfällen kann der Administrator die Ereigniskette nachverfolgen und den Absender ermitteln. Dem Vorgesetzten des Absenders kann dann eine entsprechende Meldung zugesendet werden.

SYSTEMANFORDERUNGEN

Hardware-Anforderungen:
Siehe Systemanforderungen für Microsoft Exchange Server.

Versionen von Microsoft Exchange Server:
- 2013
- 2010 x64 SP1

Betriebssysteme:
- Microsoft Small Business Server
- 2011
- 2008 Standard/Premium x64
- Microsoft Essential Business Server
- 2008 Standard/Premium x64
- Microsoft Windows Server®
- 2012 x64
- 2008 x64 R2 Standard/Enterprise Edition SP1
- 2008 x64 Standard/Enterprise Edition SP2

KS-MExchangServ/Sept14/Global

KASPERSKY lab