KASPERSKY lab

LA PROTEZIONE NEXT GENERATION PER LE E-MAIL

di e-mail vengono inviate ogni secondo.

Ne basta una per mettere a rischio la tua impresa.

Kaspersky Security for Microsoft Office 365 è pronto ad affrontare le cyberminacce 24 ore su 24

La maggior parte delle aziende ha investito tempo e fatica nella formazione degli utenti sulla minaccia delle e-mail sospette. Ma cosa si può fare quando i cybercriminali e gli spammer cambiano costantemente le loro tattiche?

Quando le e-mail sono il portatore numero uno del malware per l'azienda[1], fare affidamento sulle impostazioni di sicurezza integrate o predefinite è rischioso.

Kaspersky Security for Microsoft Office 365 aiuta l'azienda a rilevare e bloccare le e-mail nocive e di spam prima che diventino un problema, senza rallentare la produttività o eliminare accidentalmente traffico legittimo.

Come Microsoft Office 365, è ospitata nel cloud. E come tutte le soluzioni Kaspersky Lab, è basata sulla protezione più collaudata e premiata del mondo.

1: Data Breach Investigation Report (Report sull'indagine sulle violazioni dei dati) 2017 di Verizon.

Spam: più di un semplice fastidio

Dalla larghezza di banda alla perdita di produttività, lo spam è più di un disturbo aziendale: mediamente un lavoratore trascorre 13 ore all'anno scansionandolo ed eliminandolo.[2]

Cosa dire del tempo sprecato per il monitoraggio della posta aziendale legittima che è stata scambiata erroneamente per spam? La posta bloccata è una cosa, ma è ancora peggio quando la posta viene automaticamente eliminata: un problema comune con le impostazioni di sicurezza integrate nella posta su cloud.

Dobbiamo anche prendere in considerazione il fatto che molto spam porta malware. Il 58% di tutto il traffico di e-mail è spam. Perché sprecare il tempo, le risorse e il denaro controllando messaggi di posta indesiderata che nessuno vuole?

2: Atlassian: Spreco di tempo a lavoro

Tecnologie anti-spam

Kaspersky Security for Microsoft Office 365 utilizza il rilevamento e l'analisi dello spam next generation, il tutto basato su machine learning e threat intelligence in tempo reale e sul cloud di Kaspersky Security Network per rilevare e bloccare le tecniche di spam in costante evoluzione.

Anti-spam robotizzato dei contenuti

Il sistema anti-spam di Kaspersky Lab è costruito intorno a modelli di rilevamento basati su machine learning. L'elaborazione robotica dello spam viene supervisionata dagli esperti di Kaspersky Lab, consentendo il rilevamento effettivo persino dello spam sconosciuto e più sofisticato, con una perdita minima di messaggi importanti dovuta a falsi positivi.

Supporto e-mail autenticato

Spoofing è uno degli strumenti principali dello spam dannoso e fraudolento di social engineering. Sender Policy Framework (SPF) garantisce che le e-mail in entrata che sembrano provenire da fonti attendibili siano genuine, riducendo notevolmente il rischio di spoofing.

Kaspersky Security Network

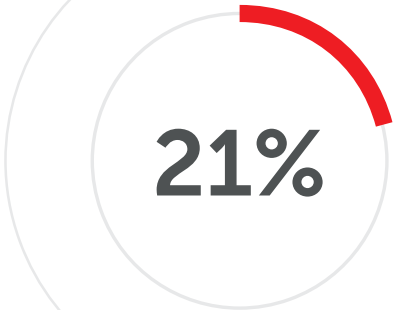
Kaspersky Security Network raccoglie quasi in tempo reale informazioni sul nuovo spam provenienti da tutto il mondo, consentendo una risposta immediata allo spam sconosciuto, compresi "zero-hour" e nuovi attacchi. Ciò avviene automaticamente, senza necessità di intervento da parte del personale IT, e aiuta a prevenire le infezioni della posta.

MassMail

I messaggi provenienti da una fonte attendibile possono avere alcuni attributi di spam senza essere effettivamente spam e possono essere persino utili a fini lavorativi. Per garantire la produttività dei dipendenti, questi messaggi possono essere contrassegnati come MassMail o spostati in una cartella speciale, anziché essere direttamente eliminati.

Phishing: la minaccia è nella posta

I cybercriminali utilizzano le e-mail per lanciare i loro attacchi perché è la strada più veloce e diretta al cuore di qualsiasi azienda.



degli incidenti segnalati implica una qualche forma di phishing[3]

I cybercriminali sanno anche che, nonostante i migliori sforzi per educare gli utenti, una e-mail ben mascherata è di solito sufficiente per convincere anche un cauto utente a cliccare su un allegato o un link dannoso. Gli attacchi di phishing comportano tipicamente e-mail mascherate come comunicazioni legittime, progettate per incoraggiare gli utenti a cliccare su un allegato o un link dannoso. Tutti li abbiamo visti: OFFERTA SPECIALE! PAGAMENTO IN RITARDO! IL VOSTRO PACCO È IN RITARDO! Queste e-mail non sono semplicemente pensate per invogliare gli utenti a cliccare senza pensare, viene deliberatamente utilizzato un linguaggio persuasivo e tecniche che le rendono convincenti.

Lo spear-phishing porta tutto questo un passo avanti. È molto più mirato e di solito individua persone scelte accuratamente che lavorano presso un'azienda con e-mail e allegati su misura che sembrano esattamente comunicazioni legittime: una "candidatura" inviata al responsabile delle assunzioni specificatamente nominato, una e-mail che fa riferimento a un reale annuncio di lavoro; una fattura inviata alla persona corretta della contabilità, facendo riferimento a un'azienda con cui fa legittimamente affari.

Più di recente, abbiamo assistito alla diffusione del "Business Email Compromise (BEC)", e-mail che sembrano provenire da qualcuno all'interno della propria azienda, come il CEO. Di solito queste "sanzionano" trasferimenti di denaro o sollecitano dati sensibili. Poiché sono personalizzate così finemente, queste e-mail riescono spesso a far cadere le vittime nella trappola dello spam: non sono inviate in grandi quantità ma sono destinate, in genere, a un paio di dipendenti ben scelti.

Nascondendo l'estensione di un file dalla vista casuale o mascherando un indirizzo e-mail in modo che sembri provenire dal CEO, i cybercriminali possono facilmente sfruttare la sicurezza debole.

3: Data Breach Investigation Report (Report sull'indagine sulle violazioni dei dati) 2017 di Verizon.

Tecnologie anti-phishing

Kaspersky Security for Microsoft Office 365 utilizza sandbox e machine learning per filtrare anche le minacce sconosciute prima che l'utente possa commettere un errore. Anche quando l'estensione di un file è nascosta, il riconoscimento del tipo di file effettivo la rileverà e la bloccherà.

Le tecnologie anti-phishing Next Generation di Kaspersky Security for Microsoft Office 365 proteggono le e-mail dalle minacce sconosciute e avanzate senza alcun impatto sulla produttività:

Motore anti-phishing basato su reti neurali

Protegge contro phishing sconosciuto e zero-hour utilizzando oltre 1000 criteri per la creazione di modelli di rilevamento. Supportato da Kaspersky Security Network, il nostro database è aggiornato continuamente dalle minacce e protegge contro URL dannosi e altre minacce correlate al phishing.

Threat intelligence basata su URL di phishing e dannosi

Supportati da Kaspersky Security Network (la nostra rete di threat intelligence basata su grandi volumi di dati, reali), i database continuamente aggiornati sono alimentati da dati scoperti automaticamente nonché dalla ricerca sulle minacce basata sull'esperienza umana.
Questo aiuta a prevenire gli attacchi drive-by e water-holing, nonché le frodi tramite siti Web dannosi.

Eliminazione, spostamento o contrassegno di messaggi di phishing

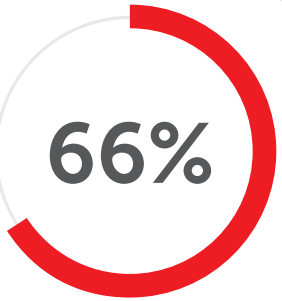
Non tutte le e-mail indesiderate sono spazzatura; la loro eliminazione automatica può causare problemi di produttività o avere un impatto sulle comunicazioni potenzialmente benefiche. L'anti-phishing di Kaspersky Lab consente il facile filtro basato su tag e tag personalizzati per contrassegnare e-mail di massa potenzialmente utili, spostandole nella cartella di posta indesiderata invece di eliminarle direttamente.

Analisi degli allegati in anteprima

Protezione contro gli attacchi di phishing avanzati che causano perdite di dati o finanziarie significative con questo sistema unico. Analizza gli allegati che possono essere visualizzati in anteprima, tra cui file PDF, RTF e MSOffice, per cercare contenuto di phishing.

Malware: ransomware, exploit zero-hour e allegati sospetti

Il 66% dei malware viene installato tramite allegati dannosi.[4] Gli attacchi zero-hour e zero-day si nascondono spesso all'interno di file Word, Excel, PowerPoint e di file di applicazioni aziendali, in attesa del clic dell'utente.

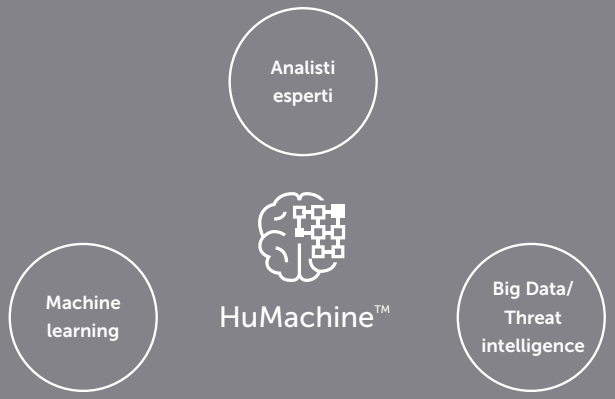


dei malware viene installato tramite gli allegati dannosi

In molti casi, gli allegati dannosi contengono malware progettato per rubare i dati di autenticazione o i dettagli di accesso utilizzando spyware: il malware viene installato senza che l'utente lo sappia. Altri attacchi comuni basati sugli allegati includono il ransomware: una volta avviato, i dati dell'utente vengono crittografati fino a quando non verrà pagato un riscatto.

Cos'è HuMachine™

HuMachine© di Kaspersky Lab combina il meglio dell'esperienza umana con la threat intelligence basata su grandi volumi di dati e con il machine learning per difendere contro ogni tipo di minaccia affrontata da un'azienda.



4: Data Breach Investigation Report (Report sull'indagine sulle violazioni dei dati) 2017 di Verizon.

Tecnologie anti-malware

Kaspersky Security for Microsoft Office 365 utilizza sandbox e machine learning per determinare la vera natura di un allegato o di un file prima che gli sia consentito di passare. I file sospetti possono essere eseguiti in uno spazio sicuro per determinare se sono un malware prima di consentirne il passaggio.

Rilevamento delle minacce a più livelli, alimentato da HuMachine

Le comprovate capacità di rilevamento delle minacce di Kaspersky Lab incorporano livelli multipli e proattivi di sicurezza che filtrano gli allegati dannosi nelle e-mail. I modelli di rilevamento basati su machine learning filtrano i malware zero-hour, precedentemente sconosciuti.

Kaspersky Security Network

La nostra rete di threat intelligence globale basata su cloud utilizza dati reali anonimi provenienti da oltre 60 milioni di sensori degli endpoint in tutto il mondo per consentire i tempi di reazione più veloci e i più elevati livelli di protezione possibili, anche mentre il panorama delle minacce evolve.

Filtro degli allegati

Bloccate i file pericolosi prima che diventino un problema e gestite i messaggi indesiderati. Il riconoscimento del tipo di file reale impedisce ai file dannosi scambiati per sicuri di passare. Il filtro degli allegati per estensione consente di bloccare o contrassegnare tipi di file indesiderati, mentre il rilevamento delle macro consente di agire su file di Office con le macro attive potenzialmente pericolose. Le esclusioni e il contrassegno flessibili aiutano a ridurre la perdita di e-mail legittime che rientrano nei criteri di filtro.

Protezione di prossima generazione conveniente, facile da gestire

Ci si trova nel cloud per convenienza, efficienza delle risorse ed efficacia dei costi. Con Kaspersky Security for Microsoft Office 365 non è necessario sacrificare nessuno di quegli elementi per la sicurezza delle e-mail. Una singola e intuitiva console di gestione consente di prendersi cura di tutto, comprese una singola vista delle minacce rilevate e le statistiche. Non vi è alcuna necessità di hardware aggiuntivo o di formazione del personale di sicurezza IT: non c'è nessun componente aggiuntivo da installare.

Inoltre, è progettato per aiutare a farlo senza rallentare o eliminare accidentalmente traffico legittimo:

Facile gestione, amministrazione e integrazione

Dashboard immediata:

Una schermata per il monitoraggio giornaliero, settimanale o mensile e stato sulle minacce, statistiche, rilevamenti, ecc.

Configurazione facile:

Tutte le impostazioni sono raggruppate in una singola schermata per la massima facilità di configurazione e di revisione.

Prova prima dell'implementazione:

È possibile scegliere quali caselle di posta elettronica proteggere, consentendo una facile prova della configurazione o un'applicazione flessibile dei criteri.

Tenancy multiple:

Attivazione di vari amministratori per gestire la soluzione utilizzando diversi account.

Backup:

Molti utenti hanno problemi con la posta legittima che viene scambiata per spam. Con meno falsi positivi e il controllo amministratore su ciò che accade alla posta sospetta, Kaspersky Security for Microsoft Office 365 riduce significativamente le possibilità che questo accada. Le e-mail eliminate vengono posizionate nei backup e possono essere cercate e ripristinate: niente più "e-mail sparite".

Notifica:

Possibilità di una rapida risposta agli incidenti con le notifiche all'amministratore per spam, phishing, attacchi virus o violazioni dei criteri.

Punto di accesso singolo:

Una console e un punto di accesso per gestire la sicurezza per diversi endpoint, dispositivi ed Exchange Online.

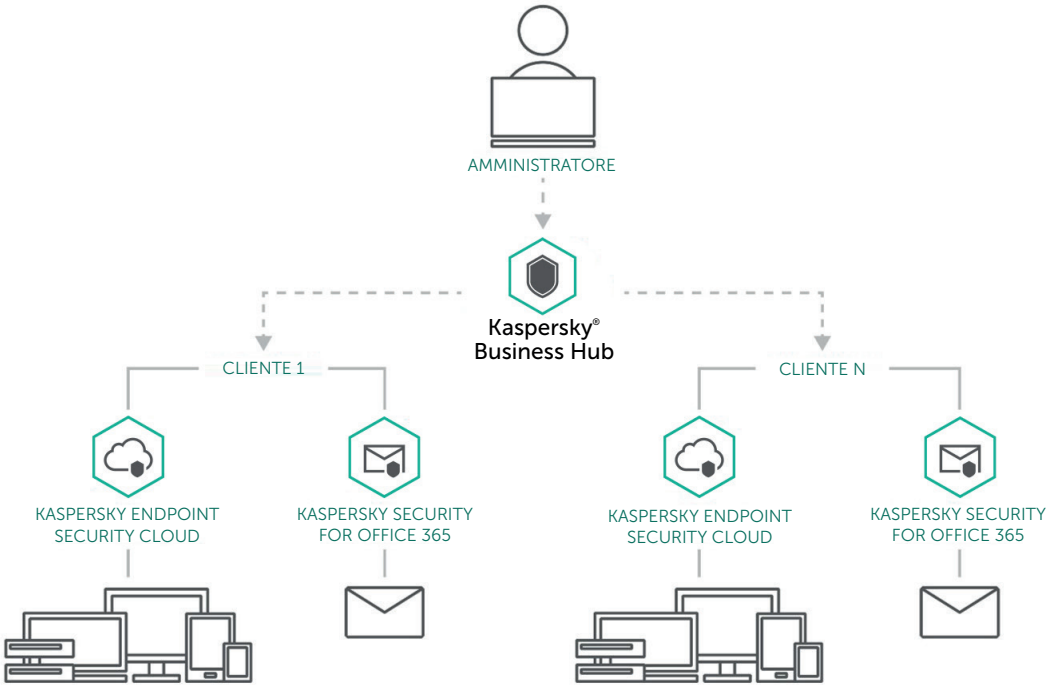
Kaspersky® Business Hub

Kaspersky Business Hub: una singola console per gestire la protezione dell'azienda.

Provate la nostra interfaccia intuitiva, la gestione semplice e la protezione superiore su differenti dispositivi e strumenti di produttività. Connessione semplice da qualsiasi dispositivo scelto: mantenete il controllo in qualsiasi momento, in qualunque luogo.

Kaspersky Business Hub gestisce i seguenti prodotti:

- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365



Kaspersky® Security for Microsoft Office 365

Quando si tratta di proteggere la propria e-mail Microsoft Office 365, la strategia migliore è assicurarsi che le minacce siano rilevate e bloccate prima che diventino un problema.

Kaspersky Security for Microsoft Office 365 è progettato per aiutare a farlo senza rallentare o eliminare accidentalmente traffico legittimo.

Scoprite in che modo le nostre tecnologie di protezione di prossima generazione possono rendere la vostra e-mail di Microsoft Office 365 ancora più facile da proteggere e gestire.

Provatelo gratuitamente su cloud.kaspersky.com