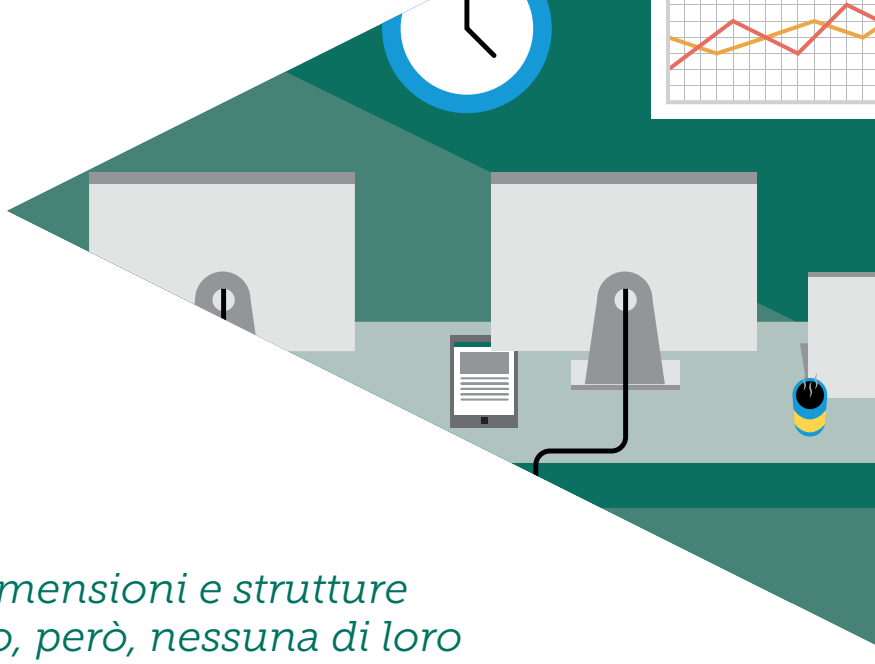
GUIDA PRATICA ALLA SICUREZZA IT PER LE PICCOLE AZIENDE

Come assicurarsi che la propria azienda abbia una protezione della sicurezza IT completa

#protectmybiz

KASPERSKY lab



Le piccole aziende hanno dimensioni e strutture diverse. Nel mercato odierno, però, nessuna di loro può permettersi di ignorare le esigenze di sicurezza online, sia che si tratti di un team che lavora per un ufficio, sia che si tratti di una persona che lavora da casa. È un problema che riguarda tutti.

Sebbene il cybercrimine spesso sia in prima pagina, in genere se ne parla quando viene colpita una grande multinazionale o un ente pubblico. I grandi numeri sono però quelli degli attacchi a privati e piccole aziende.

Solo nel 2014, sono stati rilevati 143 milioni di nuove forme di malware.[1] La maggioranza di questi attacchi era diretta a persone e organizzazioni che non si sarebbero mai considerate obiettivi probabili.

La verità è che oggi tutti possono essere un obiettivo. La buona notizia è che c'è ancora una grande differenza tra un possibile obiettivo e una vittima.

L'importante è semplicemente essere preparati. Per questo motivo abbiamo stilato questa guida: per fornire il know-how necessario a mantenere l'azienda protetta.

COS'È IL MALWARE?

Il termine malware si riferisce a programmi informatici progettati a scopi fraudolenti; in genere attaccano i dispositivi all'insaputa dell'utente. Kaspersky è leader mondiale nel rilevamento di malware, avendo ricevuto più riconoscimenti di qualunque altro fornitore di prodotti per la sicurezza.[2]

PERCHÉ HO BISOGNO DELLA PROTEZIONE?

I cybercriminali non devono arrivare a svuotare il conto bancario di un'azienda per danneggiarla economicamente. Le interruzioni provocate dal malware possono bloccare la produttività e fermare le entrate, dando luogo a una catena di effetti domino indesiderabili. Dato che è possibile proteggersi da queste eventualità con operazioni relativamente semplici, basta poco per mantenere la tranquillità.

1. AV Test
2. Tra i PRIMI 3 classificati nello Studio sui risultati di test indipendenti 2014

ELENCO DI CONTROLLO DELLA SICUREZZA

LA PRIMA OPERAZIONE DA FARE PER PROTEGGERE L'AZIENDA CONSISTE NEL CAPIRE COME SI LAVORA E VEDERE DOVE SI POSSONO RIDURRE I RISCHI. ECCO UN RAPIDO CONTROLLO DI INTEGRITÀ DELLA SICUREZZA IT:

PROTEZIONE ANTI-MALWARE ✔

Come per l'assicurazione professionale, quando si tratta di prodotti per la protezione dell'azienda, si desidera il meglio. Se non si dispone già di un software di grande efficacia che protegga i dispositivi dalle infezioni, questa deve essere una priorità.

Purtroppo, non basta fare attenzione quando si è online. Tutti sappiamo che non dobbiamo aprire allegati di mittenti sconosciuti o scaricare file da siti sospetti, ma la verità è che molte infezioni provengono da fonti attendibili che sono state compromesse.

COMPORTAMENTO NELLA NAVIGAZIONE ✔

Informare il personale sull'importanza delle azioni svolte online può prevenire molti problemi. Auspicabilmente, i dipendenti capiscono che esistono alcuni tipi di sito che non devono visitare al lavoro. Se però dispongono di un dispositivo mobile, ad esempio uno smartphone o un tablet, fuori dell'ufficio possono perdere di vista il concetto di sicurezza. Per questo è bene bloccare i siti inappropriati in modo da renderli inaccessibili dai dispositivi del posto di lavoro. La maggiore consapevolezza generale delle minacce alla sicurezza IT aiuterà i dipendenti anche a proteggersi nell'uso personale.

? IN CHE MODO POTREBBE RIGUARDARMI?

Avete mai ricevuto una email da un amico o un parente, con un collegamento interessante che, una volta aperto, sembrava sospetto? Una volta che il malware ha infettato un computer, può svolgere azioni all'insaputa dell'utente. È per questo che le fonti attendibili possono non essere sempre attendibili.

PASSWORD ✔

I dipendenti devono anche assicurarsi di usare password complesse, univoche, contenenti simboli, numeri e lettere maiuscole e minuscole. Le parole comuni possono essere forzate dalla semplice scansione di dizionari che si conclude quando si trova la parola giusta. Anche se complessa, poi, se una password già compromessa viene impiegata per più utilizzi, può portare a una violazione ancora più estesa.

AGGIORNAMENTI ✔

Ogni secondo vengono rilevati quattro nuovi malware.[3] Non si deve mai rimanere indietro. Questo significa usare gli aggiornamenti automatici per completare il software di sicurezza ogni giorno, aggiornando tutte le altre applicazioni software ove possibile, e assicurarsi che tutti coloro che lavorano nell'azienda facciano lo stesso. Non si deve dimenticare che i programmi non aggiornati sono la strada principale dei cybercriminali per attaccare le aziende.

ASSICURARSI DI NON COMMETTERE NESSUNO DI QUESTI ERRORI CLASSICI CON LE PASSWORD:

1. Uso di password facili da ricordare ma anche facili da indovinare come "password" o "123456"
2. Uso del proprio indirizzo email, nome o altro dato facilmente ottenibile come password
3. Domande per ricordare la password la cui risposta si trova facilmente: ad esempio, il nome da nubile della propria madre
4. Modifiche minime, ovvie, a parole normali, ad esempio aggiungendo un "1" alla fine
5. Uso di frasi comuni. Anche brevi frasi come "iloveyou" sono facilmente violabili

Per altri suggerimenti su come comporre password difficili da violare, vedere il post del nostro blog sull'argomento.

3 AV Test

NEL 2014

295.500

NUOVE MINACCE MALWARE MOBILI[4]

OPERAZIONI BANCARIE ✔

Dal visitare false versioni di siti attendibili all'uso di malware per spiare l'attività dell'azienda, i cybercriminali hanno numerosi metodi per ottenerne i dati finanziari. Occorre intraprendere misure attive per fermarli.

Si deve costantemente fare attenzione ai tentativi di phishing in cui i truffatori si spacciano per la banca: usare sempre un browser protetto e accertarsi di guardare bene l'URL prima di digitare i propri dati in qualunque sito. È bene anche evitare di includere nelle email tali informazioni, che potrebbero essere viste da destinatari diversi da quelli previsti.

DISPOSITIVI MOBILI ✔

Con il lavoro in movimento entrato a far parte della vita di tutti i giorni, il cybercrimine è sempre più interessato ai dispositivi mobili. Nel 2014, ogni mese sono state rilevate 295.500 nuove minacce malware mobili (scritte specificamente per smartphone e tablet).[5] Sebbene la protezione di telefoni e tablet sia importante quanto quella di Mac e PC, attualmente solo il 32% delle piccole aziende riconosce il rischio esistente per i dispositivi mobili.[6]

CRITTOGRAFIA ✔

Se si dispone di dati sensibili archiviati nel computer è necessario crittografarli, in modo che non siano utilizzabili in caso di furto o smarrimento della macchina. È importante capire che le informazioni in possesso dell'azienda sono una risorsa estremamente importante che va protetta.

? COS'È IL PHISHING?

Nel "phishing" i cybercriminali si spacciano per un'istituzione affidabile, nella speranza di ottenere informazioni come password e numeri di carta di credito da utilizzare per fini fraudolenti.

4 e 5 Secondo Kaspersky Lab
6 Indagine sui rischi IT globali per la sicurezza aziendale 2014

COMPRENDERE I RISCHI

SE SI PARLA DI SICUREZZA INFORMATICA SEMBRA TUTTO CHIARO, MA PER MOLTI DI NOI A VOLTE NON È FACILE CAPIRE QUELLO CHE PUÒ SUCCEDERE. RENDERSI CONTO DELLA CONCRETEZZA DI QUESTI PROBLEMI IN MODO DIRETTO NON È CERTAMENTE AUSPICABILE. PER QUESTO ABBIAMO TENTATO DI ILLUSTRARE IL CONCETTO USANDO DUE SITUAZIONI, LE LORO CONSEGUENZE E I MODI IN CUI SI SAREBBERO POTUTE EVITARE.

Un costosissimo caffè

Dopo aver salutato l'ultimo cliente della giornata, Tommaso lascia il suo socio a chiudere lo studio. Proprio di fronte c'è un bar, e lì ha appuntamento con un amico. Ricordando che il giorno dopo scade il termine di pagamento di un fornitore, decide di occuparsene subito, prima che gli passi di mente.

Con il laptop si connette alla rete WiFi del bar, accede al sito della banca e fa il bonifico. Contento di aver eseguito il pagamento senza ritardi, rimane seduto a prendere un meritato caffè.

Quando ripete l'accesso al conto, lo trova vuoto. Lui si arrovella tentando di capire cosa sia successo, e intanto il fornitore non è stato pagato.

COME È SUCCESSO?

Purtroppo non aveva alcuna forma di anti-malware installato e ha intercettato un keylogger dannoso. Quelli che hanno avviato il programma hanno ricevuto la registrazione di tutti i dati immessi. In più, dato che usava un WiFi pubblico non protetto, i dati della transazione erano a rischio di intercettazione.

DOVE HA SBAGLIATO?

Le operazioni bancarie devono essere eseguite solo su dispositivi dotati di anti-malware, e sempre attraverso un browser protetto. Con la funzionalità Safe Money di Kaspersky, Tommaso avrebbe potuto stabilire senza alcun dubbio se la transazione era protetta.

Vale la pena di aggiungere che utilizzando una rete pubblica non protetta i dati trasmessi erano molto più facili da intercettare che se avesse usato una connessione privata. Con una funzionalità come Safe Money installata, avrebbe però potuto avvalersi della praticità dell'online banking senza doversi preoccupare di nulla.

Email decisamente sgradite

Maria è una psicologa: ogni mattina apre la posta sul Web per trovare la conferma del prossimo appuntamento. Il primo messaggio proviene da un sito di social network che usa, e le chiede di aggiornare la password rendendola più complessa. Clicca sul collegamento, immette la password corrente quindi sostituisce una lettera sì e una no con l'asterisco.

Contenta che il suo account ora sia più difficile da violare, torna agli altri messaggi e un attimo dopo ha già dimenticato tutta la vicenda...

...finché non riceve un messaggio di ricatto con la minaccia di pubblicare i dati di tutti i clienti che ha in terapia.

COME È SUCCESSO?

Maria è stata vittima di un attacco di phishing. Sebbene il sito sembrasse quello che aveva visitato migliaia di volte, non ne era che una copia. Con l'accesso ai dati del suo profilo, erano divenuti accessibili anche quelli della sua professione. Per entrare nella sua email professionale, avevano provato a usare la stessa password che lei aveva immesso. Dato che la usava per entrambi gli account, avevano potuto leggere tutti i messaggi e i file allegati, uno dei quali era l'elenco completo dei clienti con i dati di contatto.

DOVE HA SBAGLIATO?

Innanzi tutto avrebbe dovuto sapere che organizzazioni e siti legittimi non chiedono mai i dati per email. Una volta cliccato sul link, con un buon software di sicurezza installato avrebbe ricevuto l'avviso che il sito era falso.

L'altro errore è stato quello di usare la stessa password per la posta privata e per quella professionale.

PERCHÉ SCEGLIERE KASPERSKY

LA NOSTRA MISSIONE CONSISTE NEL FORNIRE LA PROTEZIONE PIÙ EFFICACE, REATTIVA ED EFFICIENTE AL MONDO CONTRO LE MINACCE INFORMATICHE. IN KASPERSKY SMALL OFFICE SECURITY ABBIAMO UTILIZZATO LA NOSTRA COMPETENZA PER PLASMARE UNA SOLUZIONE TANTO FACILE DA USARE QUANTO UTILE, PERCHÉ POSSIATE CONTINUARE A FARE QUELLO CHE VI RIESCE MEGLIO: GESTIRE LA VOSTRA AZIENDA.

Ci rendiamo conto che, quando si tratta di sicurezza informatica, le piccole aziende sono in una posizione particolarissima. Devono affrontare le stesse minacce di tutte le imprese, e al contempo condividono molte delle stesse vulnerabilità degli utenti privati. Secondo noi questa particolare posizione ha bisogno di un approccio specifico alla sicurezza.

Cambiare l'etichetta a un prodotto per i privati proponendolo come soluzione per le piccole aziende non basta. Ad esempio, non offrirà la protezione per i server, ma molte piccole aziende ne hanno uno o dovranno introdurlo in futuro. A differenza dei privati, le aziende devono poter proteggere più dispositivi con facilità.

Non si può nemmeno togliere funzioni a una soluzione pensata per le grandi aziende: le piccole aziende non hanno né un team IT dedicato né il tempo per lottare con programmi complessi creati per gli specialisti.

Kaspersky Small Office Security è stato progettato per essere completo senza essere complicato, in modo da darvi tutta la tranquillità senza perdere risorse per dedicarle alla sicurezza. Non rallenta le prestazioni e copre una vasta gamma di dispositivi, in modo che possiate essere protetti ovunque vi troviate.

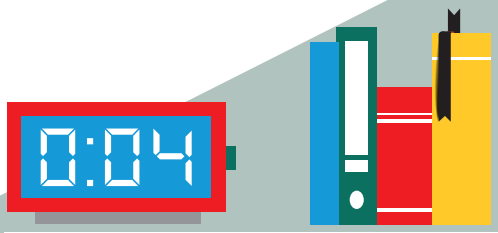
? NON POSSO USARE LA PROTEZIONE GRATUITA?

Sebbene esistano soluzioni di sicurezza gratuite, esse semplicemente non danno una protezione completa: il fatto è che lasciano deliberatamente un grosso margine di miglioramento proprio per incoraggiare gli utenti a passare alla versione a pagamento.

Quando però si tratta dell'integrità dell'azienda, bisogna avere la migliore protezione possibile, in tutte le situazioni.

COME ATTIVARSI

ORA CHE ABBIAMO IDENTIFICATO LE AREE DA INCLUDERE NEI CRITERI DI SICUREZZA, È NECESSARIO CONSIDERARE COME REALIZZARE QUESTA PROTEZIONE CON L'AIUTO DI UNA SOLUZIONE SPECIFICA.



ACCERTARSI DI ESEGUIRE REGOLARMENTE GLI AGGIORNAMENTI

Kaspersky Small Office Security è sinonimo di tranquillità: la protezione viene aggiornata automaticamente in tempo reale, mantenendo l'azienda sempre al passo con le nuove minacce non appena si presentano.

APPLICARE PASSWORD COMPLESSE

Con Kaspersky Password Manager questo è più facile per i dipendenti: genera automaticamente password complesse e le archivia in un database crittografato. Con tale funzionalità basta ricordare una sola password principale per ottenere una sicurezza molto più efficace.

CRITTOGRAFARE ED ESEGUIRE IL BACKUP DI DATI SENSIBILI/ CRITICI

Con Kaspersky Small Office Security è facile archiviare i dati critici in archivi crittografati. Con la funzione di ripristino non si possono perdere i dati essenziali, nemmeno in caso di arresto anomalo di computer o server.

INCLUDERE TUTTI I DISPOSITIVI

Kaspersky Small Office Security offre la protezione per i tablet e gli smartphone supportati. In caso di perdita o furto di dispositivi, può aiutare a individuarli e cancellare da remoto tutti i dati sensibili.

BLOCCARE I MALINTENZIONATI.

La nostra pluripremiata funzionalità Safe Money si attiva con un paio di clic e consente una navigazione super-sicura. Utilizzandola per verificare che i siti con cui si interagisce non siano stati compromessi si può prevenire istantaneamente la possibilità di violazioni. Al contempo le nostre funzionalità anti-malware, antispam e firewall tengono chiuse le porte ai criminali durante l'attività online.

PROTEGGERE L'AZIENDA, OGGI STESSO

Progettato per soddisfare le esigenze uniche delle aziende più piccole, Kaspersky Small Office Security unisce protezione avanzata e semplicità di utilizzo, essenziali per le piccole aziende.

Visitare **kaspersky.it/protectmybusiness** per scoprire come Kaspersky Small Office Security può proteggere l'azienda.

PROTEGGERE L'AZIENDA, OGGI STESSO

PARTECIPATE ALLA CONVERSAZIONE

#protectmybiz

Guardateci su YouTube

Visitate la nostra pagina Facebook

Leggete il nostro blog

Seguiteci su Twitter

Collegatevi su LinkedIn

Ulteriori informazioni sono disponibili sul sito kaspersky.it/protectmybusiness

INFORMAZIONI SU KASPERSKY LAB

Kaspersky Lab è il maggior fornitore privato di soluzioni per la protezione degli endpoint al mondo. L'azienda è tra i primi quattro fornitori mondiali di prodotti di sicurezza per utenti endpoint*. Da più di 17 anni Kaspersky Lab è pioniere della sicurezza IT e offre soluzioni efficaci per la sicurezza digitale a grandi aziende e piccole e medie imprese e a privati. Kaspersky Lab, la cui società madre ha sede legale nel Regno Unito, è attualmente presente in quasi 200 Paesi e territori a livello globale e offre soluzioni di protezione a oltre 400 milioni di utenti in tutto il mondo. Ulteriori informazioni sul sito Web: www.kaspersky.it.

* La società ha conseguito il quarto posto nella classifica 2013 di IDC relativa ai fornitori nel settore della sicurezza degli endpoint con il maggior fatturato. La classifica è stata pubblicata nella relazione di IDC dal titolo "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (IDC # 250210, agosto 2014). Nella relazione viene stilata una classifica di fornitori software basata sui ricavi ottenuti dalla vendita di soluzioni per la sicurezza degli endpoint nel 2013.