Servizio «Antivirus Dr.Web»

per le

Sommario

Preambolo

Minacce informatiche moderne

Opinione sbagliata №1

Virus vengono creati da hacker individuali

In passato, programmatori individuali creavano virus per passatempo. I programmi malevoli moderni invece vengono scritti da professionisti. Quest'è un'attività criminale ben organizzata che coinvolge sviluppatori altamente qualificati, in grado di creare programmi di sistema e applicazioni.

Struttura di alcuni gruppi criminali

In alcuni casi, gruppi criminali che sviluppano e distribuiscono malware possono includere i seguenti elementi strutturali:

1. Organizzatori — sono persone che organizzano e controllano il processo di creazione e di uso del software malevolo. Il malware può essere usato in modo immediato o venduto ad altri criminali o gruppi di criminali.
2. Partecipanti:

- Sviluppatori del software malevolo.
- Tester del software creato (fra le altre cose, si controlla se il software malevolo possa essere rilevato dagli antivirus conosciuti).
- Ricercatori delle vulnerabilità da sfruttare ai fini criminali.
- Esperti nell'uso di packer di virus e nella cifratura.
- Distributori del software malevolo, esperti nel social engineering.
- Amministratori di sistema che provvedono alla sicurezza del funzionamento distribuito dentro il gruppo criminale e alla gestione delle botnet.

Pertanto, oggi i gruppi criminali che sviluppano e distribuiscono programmi malevoli sono ben strutturati e possono produrre virus in massa. Con la crescita rapida del numero di programmi malevoli, aumentato anche il numero di firme antivirali inserite nelle basi di dati degli antivirus.

Fatti

- Il servizio di monitoraggio antivirale Dr.Web raccoglie esemplari di virus in tutto il mondo.
- Ogni giorno il laboratorio antivirale di Doctor Web riceve in media 60 000 esemplari di programmi malevoli.
- Il 28 novembre 2012 è stato una sorta di record — oltre 300 000 esemplari di virus sono stati inviati al laboratorio per essere analizzati. E con queste cifre non si esaurisce il numero di oggetti malevoli creati nell'arco di un giorno.

Gli analisti di virus non possiedono poteri magici e non possono esaminare subito diverse migliaia di file sospetti che arrivano ogni giorno. Di conseguenza, i sistemi che elaborano file sospetti in entrata diventano l'elemento più importante della protezione antivirale. La qualità di funzionamento di questi sistemi è altrettanto importante quanto la qualità di funzionamento dei prodotti commerciali in uso sui computer degli utenti.

Un antivirus deve rilevare il 100% dei virus

Spiegazione di questo sbaglio

INell'industria degli antivirus, esistono da un lungo tempo i cosiddetti test comparativi di rilevamento, svolti da tester indipendenti. Per fare questi test, si prende una raccolta di virus e malware, gli antivirus si aggiornano allo stato attuale ed eseguono una scansione della raccolta. Per vincere in un test, un antivirus deve rilevare il 100% dei virus inclusi nella raccolta.

Alcune particolarità di queste prove:

- nessun tester può garantire che la sua raccolta contenga solo programmi malevoli;
- queste prove mettono in risalto solo una delle funzioni dell'antivirus, cioè il rilevamento (individuazione) di minacce;
- queste prove valutano solo uno dei molti componenti del programma antivirale, cioè il file monitor o lo scanner, ovvero si stima la qualità di difesa contro le minacce conosciute;
- queste prove non manifestano le caratteristiche di comportamento di un antivirus in una situazione reale, né la sua capacità di curare un virus;
- queste prove non manifestano se un antivirus sia in grado di individuare minacce sconosciute.

Fatti

- Programmi malevoli, compresi i rootkit, che includono tecnologie complesse e sono molto pericolosi, si creano ai fini di lucro. Prima di rilasciarli, i loro creatori li sottopongono a test per chiarire se possano essere rilevati dagli antivirus esistenti. I cybercriminali vogliono che un malware funzioni su un computer infetto per un tempo più lungo possibile senza essere rivelato. Se un virus è facile da smascherare è quindi un virus di bassa qualità — dal punto di vista dei cybercriminali. Di conseguenza, gli antivirus potrebbero non avvistare alcuni programmi malevoli prima dell'arrivo dei relativi esemplari al laboratorio antivirale.
- Un virus può penetrare nel computer attraverso uno "0-day exploit", cioè una vulnerabilità che è ancora nota solamente allo scrittore di virus e per correggerla il produttore del software non ha ancora rilasciato una patch; oppure tramite il social engineering, in tale caso il file malevolo viene lanciato dall'utente stesso che potrebbe anche disabilitare l'auto-protezione dell'antivirus.
-

Gli antivirus catturano i virus utilizzano le firme antivirali (definizioni incluse nel database virale)

Se fosse così, l'antivirus sarebbe indifeso di fronte alle minacce sconosciute. L'antivirus però non ha cessato di essere il migliore e il più valido mezzo di protezione contro le minacce di tutti i tipi, sia **conosciute** che **sconosciute** dalla sua base di dati.

Per individuare e neutralizzare programmi malevoli sconosciuti, i prodotti Dr.Web applicano molte tecnologie di rilevamento efficaci non basate sulle firme antivirali. La combinazione di queste tecnologie permette di rivelare le minacce più recenti (sconosciute) prima dell'inserimento delle definizioni relative nella base di dati dei virus. Vediamo più nel dettaglio alcune di queste tecnologie.

- **Tecnologia Fly-Code** – assicura un controllo efficace di eseguibili pacchettati, elabora qualsiasi packer (persino un non comune) tramite la virtualizzazione dell'esecuzione del file, il che permette di rilevare virus nascosti dai packer che il software Dr.Web non conosce.
- **Tecnologia Origins Tracing** – alla scansione di un file eseguibile, il file viene considerato come un modello costruito in un modo particolare, dopo di che il modello viene comparato al database dei programmi malevoli conosciuti. Questa tecnologia è capace di riconoscere con un'elevata probabilità i virus non ancora registrati nel database virale di Dr.Web.
- **Tecnologia di analisi dell'entropia strutturale** – rileva minacce sconosciute analizzando la posizione di sezioni del codice in oggetti pacchettati e criptati, le interruzioni di funzioni di sistema e alcuni altri parametri. Il tasso di rilevamento di minacce sconosciute è molto alto.
- **Tecnologia ScriptHeuristic** – impedisce l'esecuzione di qualsiasi script dannoso nel browser e in documenti PDF, senza compromettere la funzionalità di script legittimi. Protegge dai virus sconosciuti che potrebbero infiltrarsi sul PC attraverso il browser. La tecnologia non dipende dallo stato del database virale di Dr.Web e può funzionare in qualunque browser.
- **Analizzatore euristico tradizionale** – contiene meccanismi di rilevamento dei malware sconosciuti. Il funzionamento dell'analizzatore euristico si basa sulla conoscenza (sull'euristica) di determinate particolarità (caratteri) dei virus. Tali caratteri possono essere tipici del codice virale o al contrario molto rari nei virus. Ogni carattere ha un valore – un numero il cui modulo determina la rilevanza di questo carattere e il cui segno indica se il carattere conferma o meno l'eventuale presenza di un virus sconosciuto nel codice che si sta analizzando.
- **Modulo di emulazione di esecuzione** – la tecnologia che emula l'esecuzione del codice è necessaria per individuare virus polimorfici e virus criptati compositi quando è impossibile o molto difficile applicare direttamente la ricerca per checksum (a causa dell'impossibilità di costruire definizioni affidabili). Questo metodo consiste nell'imitare l'esecuzione del codice dall'emulatore, cioè da un modello di software del processore (e parzialmente del computer e del sistema operativo).

Fatti

- L'antivirus Dr.Web ha un numero minimo di firme antivirali, perciò un solo record nel suo database virale consente di rilevare decine, centinaia e persino migliaia di virus affini. Questa è la differenza fondamentale del database virale di Dr.Web rispetto ai database degli altri antivirus: con meno record, il database di Dr.Web rende possibile il rilevamento dello stesso numero (e persino di un numero più grande) di virus e malware.
- Anche se la definizione di un virus è assente dalla base di dati di Dr.Web, questo virus verrà scoperto con un'elevata probabilità tramite molteplici tecnologie di rilevamento utilizzate dal nucleo antivirale.
- L'organizzazione dei database virali di Dr.Web è tale che la velocità di scansione non si riduce con l'aggiunta di nuove definizioni!

Grazie alla piccola dimensione del database virale di Dr.Web e a un numero di record inferiore rispetto ai concorrenti, vi sono i seguenti vantaggi:

- Risparmio di spazio su disco.
- Risparmio di memoria operativa.
- Meno traffico durante l'aggiornamento dei database.
- Alta velocità di analisi dei virus.
- Possibilità di determinare quali virus emergono in futuro tramite modifiche delle versioni esistenti.

Attenzione!

Ogni giorno milioni di persone in tutto il mondo utilizzano il prodotto unico Dr.Web CureIt! creato specialmente per curare computer compromessi su cui sono installati altri programmi antivirali.

I virus non esistono più!

È vero che oltre il 90% di minacce attuali non appartiene alla categoria dei virus nel senso stretto di questo termine perché non possiedono la capacità di replicarsi da soli (senza intervento dell'unente). La maggior parte delle minacce di oggi è cavalli di troia. I trojan sono programmi malevoli e possono causare gravi danni al proprietario del computer infetto.

I trojan pericolosi:

1. Non sono visibili né all'utente, né ad alcuni programmi antivirali.
2. Sono in grado di rubare informazioni riservate, quali password, credenziali di accesso ai sistemi di home banking e di pagamento, denaro da conti bancari.
3. Possono scaricare altri programmi dannosi e persino mettere il sistema operativo fuori servizio.
4. Possono rendere il computer completamente inutilizzabile secondo un comando dei malintenzionati.

Spesso, per un tempo dopo il rilascio, tali programmi non vengono rilevati dagli antivirus. Oltretutto, alcuni di essi cercano di rimuovere l'antivirus dal computer.

Attenzione!

Nessun altro software, **oltre all'antivirus**, è capace di curare il sistema da un trojan già attecchito.

Fatti

- I malware di oggi spesso funzionano senza farsi notare dall'utente e per un tempo dopo la creazione persino non vengono rilevati da molti programmi antivirali.
- Lo scopo degli scrittori di virus moderni è creare tali malware che avendo infettato un computer devono nascondersi per un tempo più lungo possibile e non devono essere notati né dall'utente né dai programmi speciali (antivirus).
- Per esempio, avviato sulla macchina infetta, Trojan.Carberp, creato ai fini di rubare soldi, intraprende una serie di azioni per ingannare i programmi di controllo e sorveglianza. Una volta avviato, il trojan si integra nelle altre applicazioni in esecuzione e termina il suo processo principale. In tale modo, il funzionamento successivo del trojan è suddiviso in parti ed è nascosto dentro altri processi.

È rimasta superata definitivamente l'idea che la comparsa di un virus sul computer possa essere notata.

Opinione sbagliata №5

Persino se il PC si infettasse, sarà più economico ripristinare Windows utilizzando una copia di backup che comprare un antivirus

Minaccia

Il programma malevolo potrebbe nascondersi in file custoditi in altre partizioni del disco rigido o su periferiche. In questo caso, la re-installazione di Windows non porterà ai risultati voluti perché se il file infetto verrà usato, il malware sarà attivo di nuovo.

Attenzione!

L'antivirus è il solo software che è in grado di curare un computer infettato da virus.

Anche se non avete backup di ciascuna postazione, non è un problema! Se prima dell'installazione di Dr.Web, il sistema operativo era infetto, Dr.Web lo curerà e il computer funzionerà in modo normale. Per curare un'infezione attiva, basta eseguire una scansione rapida del computer, dopodiché tutte le minacce trovate verranno neutralizzate. Per una cura di più computer della rete ci vuole meno tempo che per un ripristino del sistema operativo da una copia di riserva! Dr.Web esegue:

- la cura di file infetti;
- la correzione automatica del registro di Windows;
- la rimozione automatica di servizi malevoli;
- la rimozione automatica di rootkit e bootkit.

Opinione sbagliata №6

La fonte principale di infezione è la posta elettronica

Fatti

Le fonti principali di infezione in una rete aziendale (in ordine decrescente dei casi di infezione) sono:

- PC / notebook / dispositivi mobili personali / casalinghi dei dipendenti;
- notebook / dispositivi mobili dei clienti;
- supporti rimovibili – non sono solamente chiavette USB!
- siti consentiti (necessari per il lavoro e quindi non bloccati dall'office control) che sono stati compromessi dai cybercriminali;
- siti di phishing e siti fraudolenti appositamente creati;
- email;
- vulnerabilità dei sistemi operativi e delle applicazioni.

Panoramica dell'industria antivirale

Nella storia dell'industria antivirale è stato un periodo quando i programmatori da diversi paesi hanno cominciato a creare software chiamati con orgoglio «antivirus». Nel 1994 però è comparso il virus polimorfico Phantom-1 che solo Dr.Web poteva rivelare e a questo punto gli antivirus inefficaci hanno provato di essere inutili.

A giugno 2001 è scoppiata l'epidemia di CodeRed. Dr.Web è stato il solo antivirus nel mondo che era in grado di rivelare questo virus nella memoria del computer. Persino oggi sono pochi quegli antivirus che possono curare tali minacce.

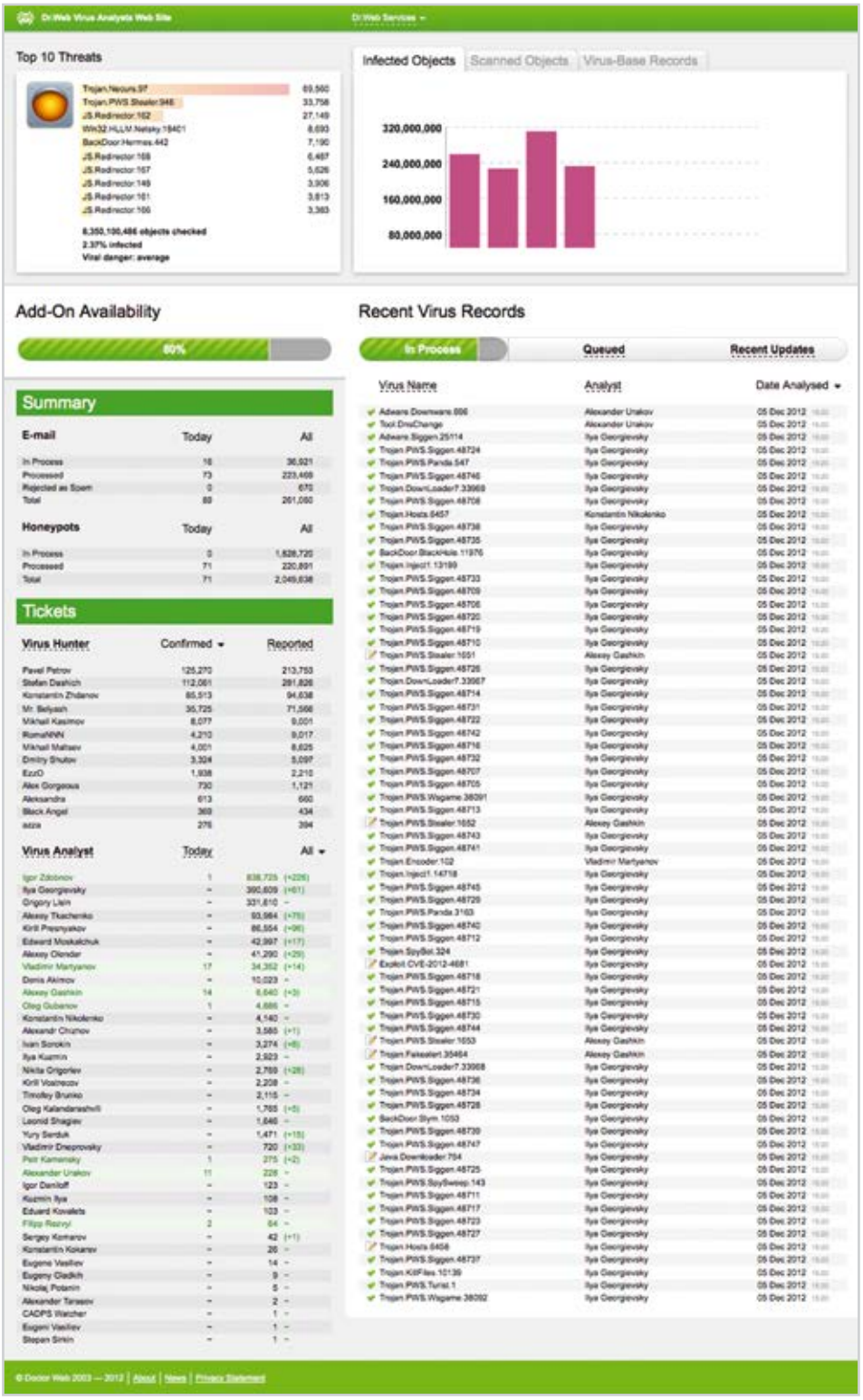
Sembra che anche adesso l'industria antivirale voglia pulirsi e liberarsi da quello che è inutile. Nel futuro resteranno sul mercato solamente quei pochi antivirus i quali:

- possono rilevare e neutralizzare virus utilizzando non solo firme antivirali e tecnologie euristiche, cioè hanno le funzioni che impediscono a un oggetto di penetrare nel sistema anche quando una definizione relativa non è ancora stata inserita nel database;
- hanno un'auto-protezione inviolabile per impedire che l'antivirus venga messo fuori servizio da un virus sconosciuto che in qualche modo si è intrufolato nel sistema;
- possono ripulire il sistema da un malware radicato se il malware è attivo, resiste, ostacola il rilevamento e nuoce all'utente, ovvero possono **curare il sistema in una situazione reale**, ripristinare il sistema al funzionamento normale, perché solo una prova in situ è capace di dimostrare se le tecnologie antivirali siano di buona qualità;
- hanno un sistema di raccolta di informazioni che trasmette velocemente al laboratorio antivirale tutte le informazioni necessarie per risolvere un problema;
- hanno un'infrastruttura potente di sviluppo, un servizio di monitoraggio dei virus, un laboratorio antivirale e un servizio di assistenza clienti;
- sanno simulare nuovi tipi di minacce prima degli scrittori di virus e utilizzare le tecnologie di difesa opportune (sicuramente quelle non basate su firme antivirali).

Tutte queste caratteristiche già sono presenti nell'antivirus moderno Dr.Web!

Sempre attivo, sempre aperto

http://live.drweb.com è una risorsa aperta che dimostra come funziona un laboratorio antivirale. Su questa pagina si può vedere come vengono esaminati esemplari di malware arrivati al laboratorio e quali virus al momento corrente sono i più diffusi.



Preambolo

La sicurezza informatica è un servizio!

L'antivirus si usa in tutti i processi d'impresa, quali la gestione aziendale, contabilità, finanze e produzione. Un antivirus efficace aiuta a rendere continui i processi d'impresa e rientra tra i fattori più rilevanti che contribuiscono alla riduzione del costo totale di possesso dell'infrastruttura IT in generale.

Come si vede dalla pratica, le aziende piccole e medie preferiscono i prodotti per i privati a tutti gli altri prodotti offerti dalle compagnie antivirali.

Quale antivirus si compra più spesso per uso aziendale? Quello migliore al mercato? Quello perfettamente adatto alle condizioni della determinata impresa? No, affatto! Si compra l'antivirus che l'amministratore di sistema dell'azienda conosce e può gestire. E anche in questo caso, l'amministratore di sistema potrebbe non usare alcune funzioni del software acquistato perché non sa come usarle o che esistono. Di conseguenza, il fondamento della sicurezza informatica dell'azienda si costruisce sulle conoscenze e sulla valutazione soggettiva di un dipendente.

Un fattore importante che impedisce il funzionamento adeguato dell'infrastruttura IT aziendale è la mancanza di amministratori di sistema qualificati. Gli amministratori IT devono essere in grado di gestire il sistema di protezione aziendale per cui sono necessarie conoscenze speciali che la maggior parte di loro non ha. Questa causa produce punti deboli nel sistema di protezione e quindi comporta l'aumento del costo totale di possesso dell'antivirus. Un'altra conseguenza è l'impossibilità di soddisfare i requisiti delle leggi riguardanti la sicurezza dell'informazione.

Questo problema è particolarmente acuto in caso di piccole e medie imprese. Di solito, le piccole e medie aziende arruolano collaboratori informatici esterni (che rendono servizi a più aziende alla volta) o assumano al lavoro amministratori con un livello di competenze inadeguato. Ridurre la dipendenza da questi fattori è un compito importante che i dirigenti dell'azienda devono affrontare.

Software come servizio (Software as a service)

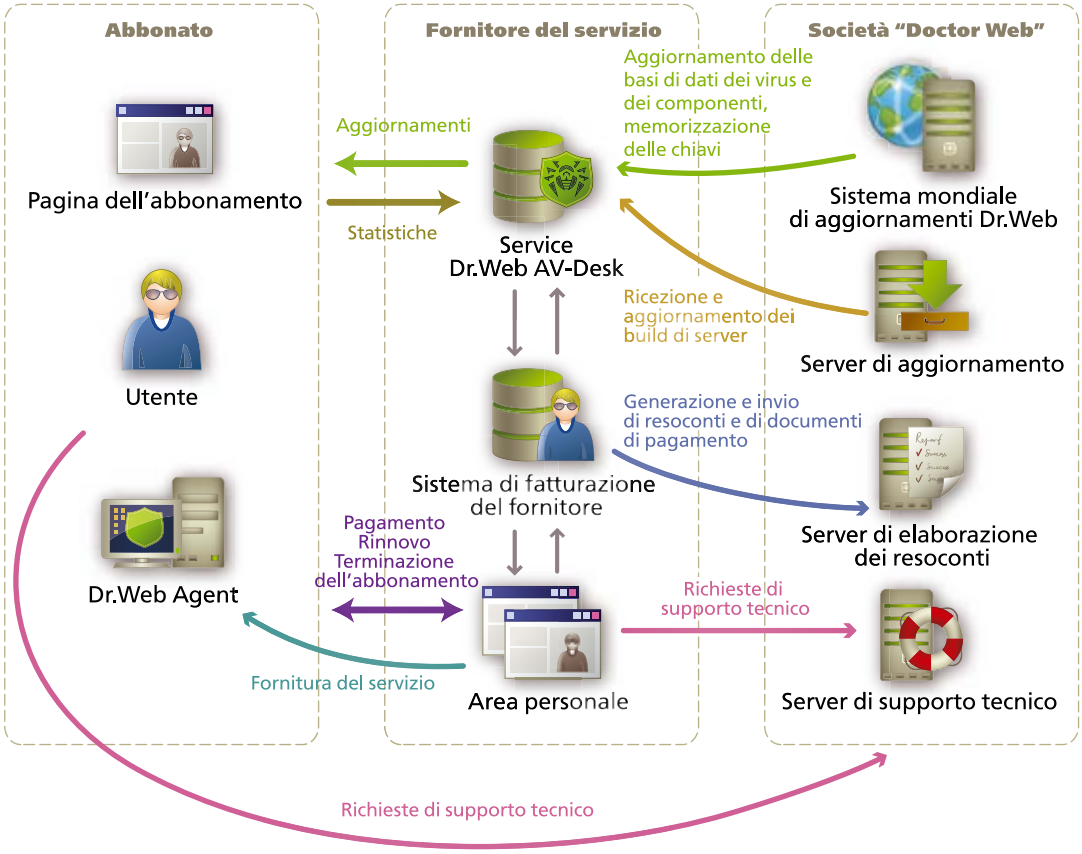
"Software as a service" ("SaaS") è un modello di distribuzione del software, ormai largamente presente, secondo il quale il software viene fornito come un servizio.

La soluzione SaaS messa a disposizione dalla società russa Doctor Web si chiama Dr.Web AV-Desk. La soluzione è stata lanciata a maggio 2007 e a quel punto era la sola in Russia. Possiamo dire che il settore di servizi antivirali è comparso al mercato russo con Dr.Web AV-Desk.

Fornitori di servizi antivirali sono ISP che hanno installato il software del web service Dr.Web AV-Desk. Tramite questo web service è possibile rendere alle aziende il servizio di protezione antivirale che si chiama "Antivirus Dr.Web".

Come funziona?

1. Il fornitore del servizio "Antivirus Dr.Web" installa il web service Dr.Web AV-Desk sui suoi server e organizza la funzione di abbonamento al servizio "Antivirus Dr.Web".
2. I clienti si abbonano al servizio, installano il software antivirale Dr.Web e gestiscono in modo indipendente i parametri del loro abbonamento.
3. La società Doctor Web mette alla disposizione del fornitore del servizio gli aggiornamenti attuali dei database virali e dei moduli del software Dr.Web e presta assistenza tecnica ai fornitori e agli abbonati.
4. Il fornitore del servizio riscuote il pagamento dal cliente, sorveglia lo stato della rete antivirale, mette aggiornamenti dei database virali alla disposizione degli abbonati e raccoglie informazioni statistiche di infezioni virali.



Se l'azienda non ha un amministratore di sistema a tempo pieno

L'utilizzo dell'antivirus Dr.Web come servizio può assicurare la protezione delle informazioni aziendali se il personale dell'azienda non include un amministratore di sistema qualificato. Se siete clienti del servizio "Antivirus Dr.Web":

- Il processo di protezione aziendale viene amministrato da specialisti altamente qualificati.
- Il personale del fornitore del servizio consiste di professionisti che hanno ottenuto certificati da Doctor Web, conoscono nel dettaglio il software il quale gestiscono e fanno il miglior uso delle loro conoscenze per gestire il sistema di sicurezza.
- Il servizio assicura che le politiche di sicurezza si osservino rigorosamente su tutti i computer aziendali — i dipendenti possono modificare solo una parte delle impostazioni dell'antivirus, oppure tali modifiche sono del tutto proibite.
- Gli specialisti del fornitore del servizio assicurano un'amministrazione corretta del software antivirale Dr.Web, una risposta adeguata alle minacce e un modo di agire professionale se si deve ripristinare la rete al funzionamento normale dopo un attacco di virus. Pertanto le spese impreviste del cliente scendono al minimo anche perché l'azienda non deve acquistare server e impiegare personale IT qualificato che prende salari alti.

L'amministrazione esterna del servizio "Antivirus Dr.Web" garantisce un funzionamento sicuro dell'infrastruttura IT dell'azienda e un'analisi spregiudicata dello stato virale della rete aziendale.

Sistema di protezione antivirale Dr.Web

Componenti di protezione antivirale

Opinione sbagliata №7

Gestione centralizzata del sistema di protezione antivirale

Se la Vostra azienda ha un amministratore di sistema a tempo pieno o ingaggia un collaboratore a progetto, il fornitore del servizio può consegnargli le funzioni che permettono di gestire il sistema di protezione antivirale tramite il Pannello di controllo. Pertanto si hanno possibilità maggiori per gestire la sicurezza della rete antivirale.

I prodotti aziendali con pannello di controllo costano di più dei prodotti per i privati. L'amministrazione di tali prodotti aziendali è molto complessa perciò si deve assumere un esperto nella sicurezza informatica

Fatti

Quando Doctor Web ha cominciato a fornire i suoi programmi di server aziendali come un servizio, ha potuto ribassare i prezzi su questi prodotti rendendoli accessibili a tutti i clienti.

Elenchiamo alcune caratteristiche del Pannello di controllo che fa parte del servizio "Antivirus Dr.Web":

1. La sua licenza è gratuita.
2. Il programma può essere gestito da un amministratore sia esperto che principiante.
3. Automatizza al grado massimo la protezione della rete locale e richiede poche spese per il supporto perché le impostazioni da applicare a ogni postazione o gruppo di postazioni si compiono in due o tre clic e possono essere modificate con facilità, se necessario.

Le funzioni del Pannello di controllo del servizio "Antivirus Dr.Web" contribuiscono al buon funzionamento dell'azienda e alla minimizzazione delle spese di procedure di business.

Il Pannello di controllo del servizio "Antivirus Dr.Web" consente di gestire la protezione di:

- postazioni Windows e Mac OS X,
- file server Windows,
- dispositivi mobili Android.

Comodo ed economico

- Il Pannello di controllo del servizio "Antivirus Dr.Web" permette di avere una "veduta aerea" dell'intera rete antivirale da una postazione. Può essere utilizzato in aziende di qualsiasi grandezza.
- Il Pannello di controllo riduce al minimo il tempo di manutenzione e consente di gestire la protezione della rete locale in qualsiasi momento e da qualsiasi luogo del mondo utilizzando un computer con qualsiasi sistema operativo. È accessibile tramite un browser perciò non si deve installare un software supplementare.
- La funzionale interfaccia web consente di installare, aggiornare e configurare componenti di protezione in maniera centralizzata, nonché accendere computer nella modalità mobile.
- Se si usa il Pannello di controllo, le risorse del calcolo delle postazioni locali subiscono un carico minore per la compressione del traffico di rete e per la cifratura dei dati, quindi le loro prestazioni aumentano rendendo gli utenti più soddisfatti.

Garantisce un elevato livello di sicurezza informatica dell'azienda

La gestione centralizzata della rete antivirale (come parte del servizio "Antivirus Dr.Web") consente di:

- realizzare le politiche di sicurezza necessarie per l'azienda impostandole in maniera centralizzata per tutte o alcune postazioni;
- garantire che i dipendenti non possano disabilitare l'antivirus o i suoi componenti sulle postazioni (tali azioni degli utenti potrebbero comportare un abbassamento del livello di protezione);
- garantire che l'antivirus abbia le impostazioni assegnate dall'amministratore della rete (non modificabili dagli utenti);
- pianificare e avviare scansioni regolari su remoto — secondo un comando dell'amministratore o secondo un calendario prestabilito;
- controllare che gli aggiornamenti si installino appena disponibili e che non possano essere disabilitati dagli utenti;
- raccogliere e analizzare informazioni concernenti lo stato della rete antivirale e generare report che si riferiscono a periodi richiesti;
- notificare gli amministratori e gli utenti dello stato della protezione antivirale;
- reagire prontamente a problemi causati dai virus: le azioni tempestive non lasciano che l'infezione si propaghi nella rete locale e riducono perdite finanziarie dell'azienda che potrebbero sorgere da eventuali periodi di inattività, perdite dei dati, assenza della connessione a Internet e infezione dei computer dei clienti.

Da notare!

- L'impossibilità di intercettare e sostituire il traffico provvede all'amministrazione sicura della rete antivirale che può consistere di un numero illimitato di postazioni locate ovunque nel mondo.

Proxy

Il servizio "Antivirus Dr.Web" è in grado di funzionare anche in una rete di una topologia complicata, per esempio, quando gli agent antivirali non hanno accesso diretto al server del servizio (al server di Dr.Web AV-Desk) e tra loro non esiste l'instradamento dei pacchetti (una rete locale interna logicamente isolata da Internet).

Per organizzare l'accesso diretto in questo caso, si può usare un componente separato della rete antivirale — il server proxy. Inoltre il server proxy può essere usato per ridurre notevolmente il traffico di rete (ottimizzazione del traffico) e per accelerare il processo di aggiornamento degli agent antivirali poiché il proxy supporta il caching.

L'utilizzo della compressione traffico (un'opzione sul server del servizio) non ostacola l'utilizzo del server proxy. Le informazioni trasmesse vengono trattate a prescindere da ciò se il traffico si comprime o meno.

Da notare!

Una rete antivirale può comprendere uno o più server proxy.

Installazione via rete (installazione remota)

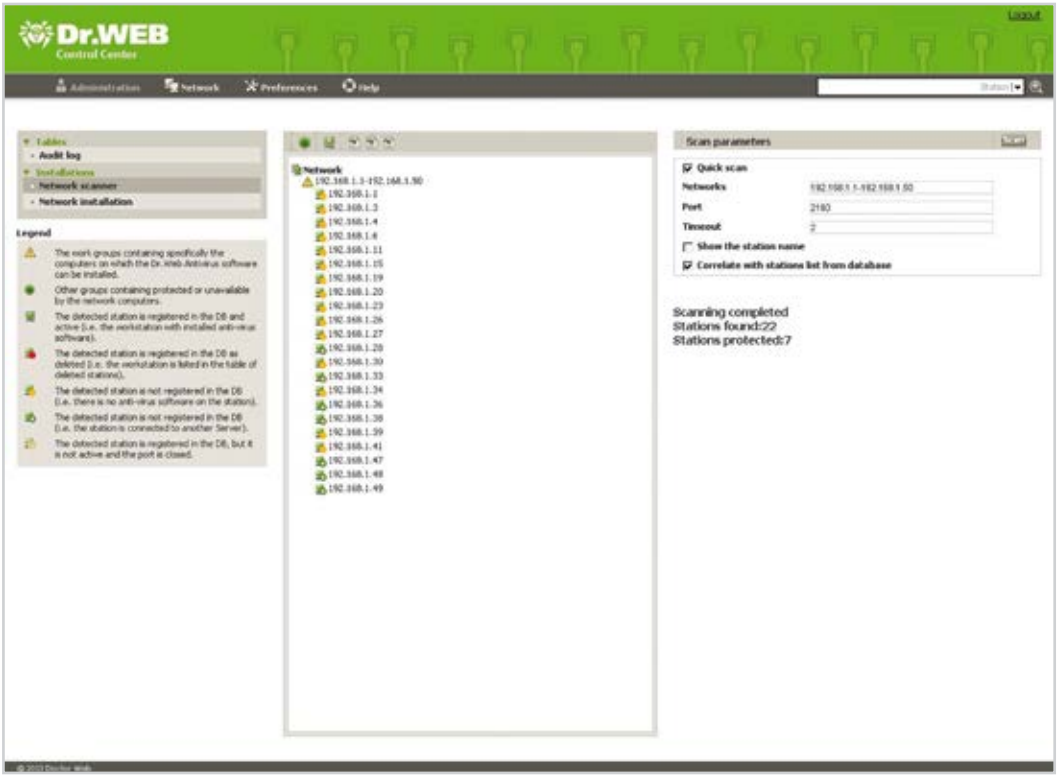
Il servizio "Antivirus Dr.Web" presenta tutti i vantaggi che hanno i prodotti di classe "enterprise" con gestione centralizzata. Uno di questi vantaggi è la possibilità di individuare nella rete locale nodi non protetti dal software antivirale e quindi di installare Dr.Web su tali computer tramite un'installazione su remoto.

L'installazione remota è possibile sia nel caso in cui la postazione fa parte del dominio con l'account di amministratore che nel caso in cui la postazione non è inclusa nel dominio o si usa un account locale.

Attenzione!

Se la postazione remota non fa parte del dominio o su di essa si usa un account locale, sarà necessario eseguire alcune impostazioni in caso di alcune versioni del SO MS Windows. Le impostazioni sono descritte nel Manuale dell'amministratore.

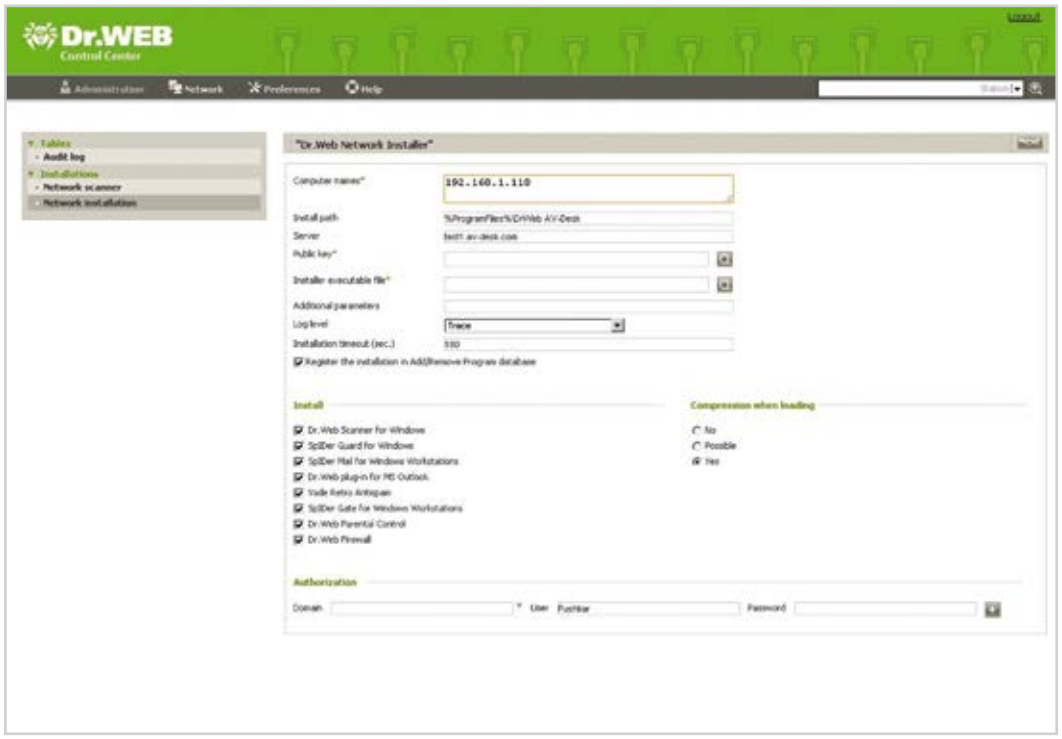
Il Pannello di controllo del servizio "Antivirus Dr.Web" comprende lo Scanner di rete che cerca computer nella rete locale per indirizzi IP. Come risultato, restituisce un elenco gerarchico dei computer segnalando su quali computer l'antivirus è installato e su quali no.



L'antivirus può essere installato su una o più postazioni remote non protette creando un task relativo nella barra degli strumenti.

Attenzione!

L'installazione remota è possibile ESCLUSIVAMENTE nelle reti con routing.



Amministratori del sistema antivirale

Se l'azienda ha un amministratore di sistema a tempo pieno o ingaggia un collaboratore a progetto, loro possono gestire il sistema di protezione antivirale Dr.Web tramite il funzionale e intuitivo Pannello di controllo. L'amministratore può controllare l'osservazione delle politiche di sicurezza aziendali e reagire prontamente a incidenti provocati da programmi malevoli, cioè può avere tutti i poteri necessari per gestire la protezione antivirale dell'azienda in modo appropriato.

Tipi di amministratori

- **Amministratore di gruppi con pieni diritti** – può accedere al Pannello di controllo e modificare tutte le impostazioni del sistema di protezione antivirale. Si consiglia di assegnare i pieni diritti a un dirigente (se l'azienda è piccola, non impiega un addetto informatico e il dirigente svolge anche il ruolo di amministratore del sistema di protezione antivirale), oppure all'addetto informatico autorizzato all'amministrare il sistema di protezione antivirale.

Attenzione!

Se l'azienda arruola un collaboratore informatico esterno, si deve valutare se sia affidabile e se gli possano essere consegnati tutti i privilegi di amministrazione del sistema di protezione antivirale.

- **Amministratore di gruppi con pieni diritti (sola lettura)** – può accedere al Pannello di controllo e ottenere dati statistici del sistema di protezione antivirale, ma non può modificare le impostazioni. Questo profilo può essere assegnato a un dipendente che deve analizzare dati statistici e condurre verifiche del sistema di protezione antivirale.
- **Amministratore di gruppi con diritti limitati** – può accedere al Pannello di controllo e modificare le impostazioni che corrispondono ai permessi assegnatigli "dall'amministratore di gruppi con pieni diritti", eccetto le funzioni di gestione degli abbonamenti (creare / sospendere / rinnovare / rimuovere un abbonamento). Questo profilo può essere utile per 1) i clienti dei fornitori del servizio "Antivirus Dr.Web" in outsourcing e 2) gli amministratori degli abbonati degli ISP. Se vi sono più gruppi, un amministratore separato può essere designato per ciascun gruppo.

Importante!

Se si vogliono designare amministratori del sistema, si deve avere l'accesso alle funzioni corrispondenti. Per ottenere l'accesso, rivolgeteVi al Vostro fornitore del servizio "Antivirus Dr.Web".

Gruppi. Gestione dei gruppi

Nelle aziende medie e grandi, per facilitare l'amministrazione del sistema di protezione, si può usare la funzione di raggruppamento che rende il servizio "Antivirus Dr.Web" molto scalabile. Il raggruppamento consente di:

- creare gruppi, riunire postazioni in gruppi, aggiungere una postazione a un gruppo o rimuoverla dal gruppo;
- applicare diverse politiche di sicurezza a diversi gruppi (per esempio, si determina che il gruppo "Contabilità" non possa annullare aggiornamenti dell'antivirus, mentre il gruppo Manager abbia poche limitazioni nell'usare Internet);
- assegnare task con un singolo comando a tutte le postazioni di un gruppo e lanciare l'esecuzione dei task sulle postazioni;
- impostare per i gruppi calendari individuali di aggiornamenti e di scansioni ai fini di distribuire il carico della rete;
- generare report per gruppo;
- inviare avvisi a singole postazioni, ad alcuni gruppi o a tutti i gruppi.

Se un'azienda ha più di quindici abbonamenti al servizio "Antivirus Dr.Web", è opportuno creare gruppi nel sistema di protezione e applicarci diverse politiche di sicurezza utilizzando le abbondanti impostazioni del Pannello di controllo.

L'amministratore di sistema può ampliare o limitare i diritti di gestione agent assegnati a singoli utenti, a un gruppo o a tutti i gruppi. È possibile:

- consentire di modificare le impostazioni dell'agent;
- limitare parzialmente il diritto di modificare le impostazioni;
- proibire completamente la modifica delle impostazioni;
- gestire componenti Dr.Web installati sulle postazioni;
- installare / rimuovere componenti Dr.Web sulle postazioni;
- avviare task sulle postazioni;
- aggiornare in modo forzato gli agent che non si aggiornavano da un lungo tempo;
- avviare forzatamente una scansione che si esegue in background sulle postazioni.

Pacchetti di tariffa e componenti di protezione Dr.Web

Il cliente può abbonarsi al servizio scegliendo uno dei pacchetti di tariffa. Ogni pacchetto di tariffa include moduli di protezione da utilizzare su postazioni, file server Windows e dispositivi mobili.

Scegliete quei pacchetti di tariffa che rispecchiano le esigenze della Vostra azienda! Prendete in considerazione i requisiti della sicurezza informatica e lo stato finanziario attuale dell'azienda.

	Dr.Web Classico Protezione indispensabile contro i virus	Dr.Web Premium Protezione completa contro le minacce provenienti da Internet
Protezione di postazioni		
Windows	8/7/Vista/XP	
Mac OS X	10.4 o superiore	
Antivirus, antispyware, antirootkit	✔	✔
Antispam		✔
Monitoraggio HTTP		✔
Parental control		✔
Firewall	✔	✔
Protezione di file server		
Windows		Windows Server 2003/2008
Protezione di dispositivi mobili		
Android		2.0/2.1/2.2/2.3/ 3.0/3.1/3.2/4.0/4.1/4.2
Antivirus	✔	✔
Antifurto		✔
Antispam		✔
Supporto tecnico base		
Aggiornamenti dei database virali	✔	✔
Aggiornamenti dei componenti di Dr.Web	✔	✔
Numero di richieste di supporto tecnico	Nessun limite	
Altri servizi		
Passaggio gratuito a un altro pacchetto di tariffa	✔	✔
Sospensione dell'abbonamento (per 1, 2 o 3 mesi)	✔	✔

Da quali minacce protegge il servizio “Antivirus Dr.Web”?

	Dr.Web Classico	Dr.Web Premium
Virus	✔	✔
Cavalli di troia	✔	✔
Keylogger	✔	✔
Password stealer	✔	✔
Spyware	✔	✔
Rootkit	✔	✔
Riskware	✔	✔
Virus polimorfici	✔	✔
Worm	✔	✔
Backdoor	✔	✔
Joke	✔	✔
Paid dialer	✔	✔
Hacktool	✔	✔
Spam		✔
Phishing		✔
Pharming		✔
Scamming		✔
Spam tecnico (bounce)		✔
Furto delle informazioni riservate		✔
Cybercriminalità diretta contro i minori		✔
Accesso non autorizzato tramite la rete	✔	✔

Solo un antivirus non basta!

Perché oggi non basta usare un mero antivirus? Non era così nel passato!

Attenzione!

Il sistema di protezione antivirale moderna non è uguale al file antivirus di ieri.

Oggi un sistema di protezione antivirale deve comprendere tra le altre cose:

- un antispam efficace poiché lo spam è uno dei veicoli principali che trasportano programmi malevoli;
- uno strumento di monitoraggio del traffico HTTP che protegge il computer da codici dannosi provenienti da siti web;
- la possibilità di restringere l’accesso a periferiche e risorse locali (Parental control od Office control);
- un firewall personale.

Attenzione!

Tutte queste funzioni sono incluse solo nel pacchetto di tariffa Dr.Web Premium.

Se questi componenti di protezione si usano correttamente (nel rispetto delle raccomandazioni di quest’opuscolo), si esclude la necessità di acquistare in aggiunta altri programmi con le funzioni simili. Pertanto, è possibile implementare un sistema di protezione antivirale a costi moderati.

Best practice

- Configurando nel Pannello di controllo gli accessi degli utenti ai componenti antivirali, consentite agli utenti di avviare ciascuno dei componenti, ma vietate loro di modificare le impostazioni e di fermare i componenti.
- Va IGNORATA l'opinione del dipendente su quali componenti di protezione antivirale devono essere installati sul suo computer.

Si paga solo per quello che si utilizza

"Il cliente paga solo per quei componenti di protezione che gli servono al momento" — questo è il principio fondamentale di concessione licenze del servizio "Antivirus Dr.Web". Si può decidere quale protezione sia opportuna in ogni momento. **Il cliente paga sempre per il numero effettivo di abbonamenti, e questo numero può cambiare flessibilmente sia in alto che in basso.**

Grazie a questa filosofia, la Vostra azienda può pianificare con precisione le spese di sicurezza informatica a breve e a lungo termine tenendo conto delle sue esigenze reali. La flessibilità del servizio esclude un aumento non previsto di spese e permette di capire quanto e per che cosa si dovrà pagare in futuro.

Vantaggi di concessione di licenze del servizio "Antivirus Dr.Web"

- Il periodo minimo di tariffazione è di un mese. Il cliente deve pagare solo per gli abbonamenti attivi di fatto nel periodo di riferimento.
- Nuove postazioni si aderiscono al servizio appena necessario.
- Se il numero di dipendenti decresce, le postazioni non utilizzate si disconnettono dal servizio.

Potete abbassare le Vostre spese di sicurezza informatica quando usate meno abbonamenti e accrescerle quando il numero di abbonamenti aumenta con il progresso dell'impresa.

Sconti

AbbonandoVi al servizio "Antivirus Dr.Web", cominciate a risparmiare sulla sicurezza informatica dal primo mese di uso.

AbbonateVi al servizio e ottenete sconti concessi …

per il numero di oggetti protetti ...

dal 10 al 40 % — secondo il numero di oggetti protetti inclusi nell'abbonamento.

Numero di PC	Sconto, %
1–25	Prezzo base della tariffa
26–50	10
51–100	20
101–200	25
201–300	30
301–400	35
401–500	40

... e per il tempo di uso del servizio

dal 5 al 15 % — uno sconto speciale concesso in aggiunta agli abbonati che hanno usato il servizio senza interruzioni*

Durata di abbonamento	Sconto, %
1 anno	5
3 anni	10
5 anni	15

** Senza sospensione o annullamento dell'abbonamento. Lo sconto si conteggia dal 13°, 37° e 61° mese rispettivamente*

Le licenze flessibili del servizio offrono una reale possibilità per risparmiare sulla sicurezza informatica.

Pannello di controllo degli abbonamenti

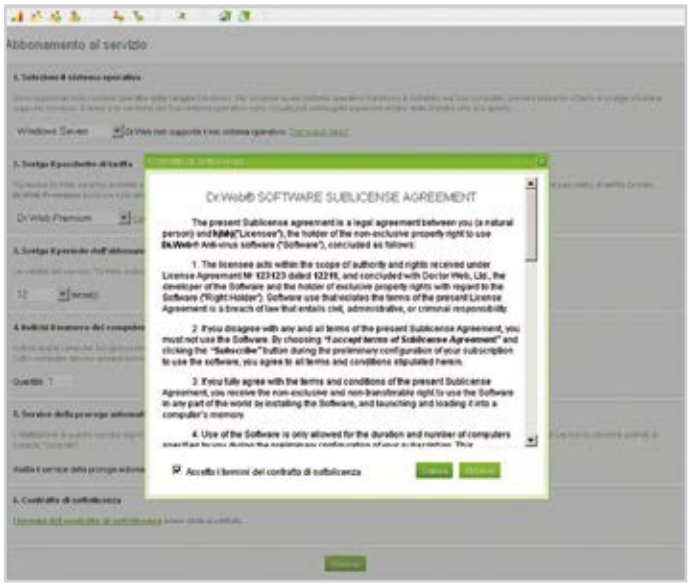
Il cliente può accedere al Pannello di controllo degli abbonamenti dopo che il fornitore del servizio gli ha consentito l'accesso opportuno. Tramite il Pannello di controllo, il cliente può gestire i suoi abbonamenti, rinnovarli, passare ad altri pacchetti di tariffa, ottenere statistiche sui virus e sul funzionamento del servizio, ricevere in tempo reale notizie di Doctor Web e fare richieste di supporto tecnico.

Abbonamento

Nel Pannello di controllo dell'abbonamento, il cliente può connettere nuove postazioni al servizio (ampliare la licenza) o disconnettere le postazioni superflue quando il numero di computer usati dal personale diminuisce.

Per abbonarsi, è necessario eseguire le seguenti azioni:

1. Indicare il sistema operativo in uso.
2. Scegliere un pacchetto di tariffa.
3. Indicare il numero di computer.
4. Indicare il tempo di abbonamento (il periodo minimo è di un mese).
5. Accettare i termini del contratto di sublicenza.
6. Premere sul tasto "Abbonarsi".



Da notare!

Il flag "Il servizio di rinnovo automatico è attivo" deve essere spuntato — in tale caso l'abbonamento si rinnoverà ogni mese successivo in modo automatico.

Installazione del software del servizio sulle postazioni

Subito dopo l'effettuazione dell'abbonamento, nel Pannello di controllo abbonamenti diventa disponibile un collegamento al pacchetto di installazione di Dr.Web. Si deve scaricare il pacchetto di installazione, lanciare il file e attendere fino a quando l'installazione di Dr.Web si compia. Alla fine dell'installazione, un'icona verde con il ragno appare nell'angolo inferiore destro dello schermo e sull'icona si lampeggia un triangolo giallo con il punto esclamativo. È necessario riavviare il computer e attendere fino a quando l'agent Dr.Web si connetta al server antivirale. A questo punto la postazione è stata connessa al servizio.

Attenzione!

1. Prima di installare il software Dr.Web, si deve accertarsi che nessun altro programma antivirale sia installato sul computer poiché i moduli residenti possono portare all'incompatibilità dei programmi.
2. La protezione antivirale Dr.Web comincia a funzionare dopo l'installazione del software del servizio "Antivirus Dr.Web".

Rinnovo dell'abbonamento

Non è necessario prendersi cura del rinnovo. L'abbonamento si rinnova automaticamente se al momento quando ci si abbona, non è stato deselezionato il flag "Il servizio di rinnovo automatico è attivo".

Sospensione dell'abbonamento

Se necessario, l'abbonamento può essere sospeso in qualunque momento. La sospensione può durare fino a 3 mesi.

Per sospendere l'abbonamento, selezionate la voce "Sospendere abbonamento" nella scheda "Gestione".

Attenzione!

Se sospendete il Vostro abbonamento, non avrete più il diritto agli sconti cumulativi concessi per il tempo di uso del servizio (vedi la sezione Sconti).

Quando comincia il periodo di sospensione?

- In caso di tariffazione giornaliera — dal giorno di sospensione.
- In caso di tariffazione mensile — dal primo giorno del mese di calendario successivo.

Quando finisce il periodo di sospensione?

- Trascorso il periodo di sospensione impostato. Allo stesso tempo si abilita il servizio di rinnovo automatico, se l'avete attivato prima di sospendere l'abbonamento.

Rinnovo automatico dell'abbonamento dopo la sospensione

Avviene se il servizio di rinnovo automatico è stato attivato prima della sospensione dell'abbonamento. L'abbonamento si rinnova alle stesse condizioni che erano in vigore prima della sospensione.

Interruzione dell'abbonamento

Il cliente può disdire l'abbonamento in qualsiasi momento. In tale caso:

- se la tariffazione è giornaliera, l'abbonamento si interrompe subito;
- se la tariffazione è mensile, l'abbonamento rimane attivo fino alla fine del mese di calendario corrente. I fondi versati in anticipo e non spesi al momento di interruzione dell'abbonamento non vengono risarciti.

Per interrompere l'abbonamento, selezionate la voce "Annullare abbonamento" nella scheda "Gestione".

Rinnovo manuale dell'abbonamento dopo l'annullamento

L'abbonamento si rinnova dopo che è stata selezionata l'azione "Rinnovare abbonamento". Diventa disponibile un collegamento per scaricare il pacchetto di installazione di Dr.Web. In realtà, questo è un nuovo abbonamento. Allo stesso tempo si abilita il servizio di rinnovo automatico, se l'avete attivato prima di sospendere l'abbonamento.

Selezionate la voce "Rinnovare abbonamento" nella scheda "Gestione".

Certificato di autenticità online

Il certificato di autenticità Dr.Web può essere generato nel Pannello di controllo dell'abbonamento. Il certificato di autenticità convalida che il software Dr.Web si usa in modo legittimo.

Informazioni statistiche

Il Pannello di controllo dell'abbonamento può generare vari report di attività eseguite dall'antivirus sulle postazioni protette. Pertanto, il software del servizio funziona in maniera trasparente dal punto di vista dell'utente.

Si possono conoscere parametri di ciascun abbonamento e di ogni gruppo di abbonamenti e avere le informazioni complessive su tutti gli abbonamenti. In qualunque momento (anche quando un abbonamento è sospeso) il cliente può controllare lo status dell'abbonamento, i dati di ciascun abbonamento o di tutti gli abbonamenti, i progressi degli abbonamenti (secondo i gruppi e le tariffe).

Statistiche di virus

La scheda "Statistiche" mette alla disposizione le informazioni riguardanti virus e programmi malevoli trovati dall'Antivirus Dr.Web sui computer protetti. Le informazioni si presentano in forma visiva in diagrammi e classificazioni.

Per ogni postazione e per qualsiasi periodo (impostabile), si visualizzano:

- dati aggregati di minacce trovate dall'antivirus Dr.Web;
- i dieci virus più diffusi.

Log di azioni

Il log presenta le informazioni esaurienti (storia) delle azioni eseguite dal cliente nel Pannello di controllo dell'abbonamento:

- azioni del mese corrente eseguite con ciascun abbonamento e con tutti gli abbonamenti (effettuazione dell'abbonamento, annullamento dell'abbonamento, sospensione, entrate nell'area personale di utente ecc.);
- azioni del mese corrente eseguite con il conto personale del cliente (accrediti, addebiti, rimborsi).

Sistema di protezione antivirale Dr.Web

Politiche di sicurezza informatica

Creazione di un sistema integrato di protezione

L'esperienza mostra che le postazioni e i server sono i punti più vulnerabili di una rete locale. Proprio da essi si propagano i virus e spesso anche lo spam.

I virus possono penetrare sui computer in svariati modi: da schede di memoria flash, da archivi protetti da password allegati a email che hanno sfuggito al controllo sul server, da siti web infetti su quali si è passati utilizzando collegamenti ricevuti in email.

Secondo i principi moderni della sicurezza informatica, la protezione antivirale di ogni postazione deve comprendere un antivirus efficace e uno strumento di limitazione di accesso a risorse locale che serve per evitare accessi intenzionali o accidentali ai dati e per escludere inconvenienti nel funzionamento del sistema.

È un errore comune pensare che si debbano proteggere solo le postazioni e i server Windows perché esistono pochi malware per Linux e Unix. Come risultato di tale "politica di protezione", i malware si insediano sulle macchine non protette. Anche se i malware non possono infettare i sistemi operativi e le applicazioni in esecuzione, essi possono usarli come fonte di infezione, per esempio, infettando altri computer tramite cartelle condivise ad accesso aperto.

Da notare!

Tramite il Pannello di controllo del servizio "Antivirus Dr.Web", si può controllare in modo centralizzato il sistema di protezione antivirale su qualsiasi numero di computer Windows e Mac OS X.

Obiettivo №2

Protezione del file server

Minaccia

Di solito, le aziende proteggono soli computer di ufficio e lasciano non protetti server, dispositivi mobili e computer casalinghi dei dipendenti. Di conseguenza, se un malware si è infiltrato su una postazione, può facilmente infettare i server che contengono informazioni critiche.

Perché è importante proteggere i server?

- L'utente potrebbe far entrare sul server un virus non conosciuto al momento di infezione (portandolo o lanciandolo dal repository). L'antivirus installato sul server catturerà subito il virus adoperando le sue tecnologie euristiche. Nel caso pessimo, l'antivirus curerà il virus dopo il successivo aggiornamento dei database virali.
- Il server potrebbe essere violato da pirati informatici. L'antivirus installato non lo permetterà poiché rivelerà ed eliminerà i programmi malevoli. Se il server è coperto dalla gestione centralizzata, l'amministratore riceverà subito un avviso che riferisce un cambio dello stato di postazione (per esempio, un tentativo di fermare il sistema di protezione).
- Il mondo odierno è pieno di tecnologie digitali. Utenti possono lavorare non solo in ufficio, ma anche a casa, e possono memorizzare dati sui file server aziendali e anche sui server nella Rete. Utenti collegano al computer i loro dischi di memoria flash e anche quelli degli amici e dei colleghi. Questi supporti potrebbero contenere virus.
- I cellulari moderni hanno sistemi operativi e applicazioni e di conseguenza, come i desktop, possono essere infettati da malware. Se connessi alla rete aziendale, i cellulari ci portano i virus presenti su di essi i quali potrebbero arrivare anche sul server.

Best practice

Se la Vostra azienda ha un file server dedicato, anch'esso deve essere protetto.

Soluzione

Per proteggere il file server, conviene usare il pacchetto di tariffa Dr.Web Premium che supporta Microsoft Windows 2003/2008.

Se per proteggere il server si usa il servizio "Antivirus Dr.Web", il costo di protezione sarà quello di protezione delle workstation e quindi si paga molto di meno rispetto ai prezzi dei soliti prodotti antivirali per server. Anche questo è uno dei molteplici vantaggi del servizio "Antivirus Dr.Web".

Da notare!

Tramite il Pannello di controllo del servizio "Antivirus Dr.Web", si può controllare in modo centralizzato il sistema di protezione antivirale su file server Windows di un numero illimitato.

Protezione dei dispositivi personali dei dipendenti

Oggi molti dei computer che si trovano nell'ufficio di un'azienda appartengono non ad essa, ma ai dipendenti — sono i loro notebook e smartphone personali. I professionisti appassionati lavorano nell'ufficio, ma anche strada facendo e a casa. Rimangono sempre raggiungibili e talvolta sacrificano le ore di riposo. Tale approccio al lavoro, diventato possibile grazie alle nuove tecnologie, viene apprezzato dalle aziende. Inoltre molte imprese impiegano personale che lavora su remoto, il che può comportare risparmi importanti.

Tuttavia a ciascun vantaggio si associa una sfida, ovvero si deve pagare per tutto. Prima l'azienda poteva sempre garantire che la protezione della rete locale rimanga sul livello richiesto perché gli amministratori di sistema controllavano ogni computer nella rete aziendale. Con la nuova organizzazione del lavoro, questo non è più possibile.

Rischi

- Quasi due terzi dei dipendenti (63,3%) possono accedere alle informazioni aziendali su remoto dai loro dispositivi personali, compresi smartphone.
- Nel 70% dei casi, i virus entrano nelle reti locali dai dispositivi personali (notebook, netbook, ultrabook, palmari, cellulari) e dai supporti rimovibili (chiavette USB) dei dipendenti.

- Il 60% dei computer casalinghi non ha nessuna protezione contro i virus! Ciò vuol dire che fuori ufficio i dipendenti usano elaboratori che non sono protetti da attacchi di hacker, potrebbero contenere virus e trojan e consentire ai malintenzionati di sfruttare le vulnerabilità del software. Accedendo da tali computer, i dipendenti mettono a rischio la rete aziendale.
- Pertanto esiste il rischio che le informazioni importanti dell'azienda possano essere rubate, sostituite o compromesse.

Fatti

Pur essendo professionisti nel loro campo, i dipendenti potrebbero non conoscere a sufficienza i principi di sicurezza informatica e persino potrebbero avere idee false al riguardo.

È nell'interesse dell'azienda assicurare la protezione di tutti i dispositivi utilizzati dai dipendenti, a prescindere dal proprietario del dispositivo e dal luogo dove si trova.

A tale scopo conviene adoperare uno strumento che può garantire:

- la protezione di qualsiasi informazione sui dispositivi degli utenti;
- l'impossibilità che i virus e trojan si propaghino dai dispositivi degli utenti;
- la protezione per computer di ogni tipo, compresi cellulari — perché se un dispositivo rimane senza protezione, esso potrebbe essere sfruttato dai cybercriminali per penetrare nella rete.

Però i dipendenti usano dispositivi privati anche ai fini personali!

I fini personali potrebbero essere i seguenti: si permette al figlio di usare il notebook, si trascorre la serata in un social network infestato dai virus, si scaricano filmati e brani da un sito inaffidabile e così via. Che tipo di sicurezza delle informazioni aziendali è qui!

Con il servizio "Antivirus Dr.Web" si può fare quasi l'impossibile — si può proteggere ogni dispositivo in un modo conveniente per tutti, sia per l'azienda che per i dipendenti.

Best practice

- Acquistate un abbonamento al servizio "Antivirus Dr.Web" per i dispositivi personali dei vostri dipendenti — in tale caso tutti i computer che hanno accesso alla rete aziendale avranno una protezione provvista dallo stesso fornitore.
- Tramite il Pannello di controllo del servizio, assicurate che le politiche di sicurezza dell'informazione vengano osservate anche sui dispositivi personali dei vostri dipendenti. In particolare, si può impostare che gli utenti non possano disabilitare aggiornamenti, annullare scansioni regolari e rimuovere componenti di protezione.
- Si deve TRASCURARE l'opinione del dipendente sulla scelta dell'antivirus da installare sul suo dispositivo personale fino a quando tale dispositivo rimanga incluso nella rete aziendale. Altrimenti, tale dispositivo deve essere annunciato inattendibile e ad esso deve essere negato l'accesso alla rete aziendale.

Soddisfatte queste condizioni, si può garantire che i programmi malevoli non si intrufoleranno nella rete aziendale dai computer personali dei dipendenti.

Vantaggi per l'azienda

- Dedizione del personale. Un antivirus gratuito è un ottimo bonus!
- Si riduce il costo di organizzazione della protezione.
- Tutti i computer nella rete antivirale possono essere controllati da una singola postazione.
- I dipendenti possono lavorare ovunque ed essere ugualmente protetti.
- In qualsiasi momento si garantisce la sicurezza delle informazioni (anche di quelle personali).
- Riduzione dei casi quando il lavoro si ferma a causa di incidenti virali.

I dipendenti hanno da lungo superato il perimetro della protezione aziendale, non è possibile farli tornare indietro e non vale la pena di farlo. Sarà più saggio allargare i confini della protezione e includerci lo spazio personale di ogni dipendente.

Protezione dei dispositivi mobili — quelli dell'azienda e dei dipendenti

I dispositivi mobili più diffusi funzionano sulla base del SO Android.

Rischi

- Il numero di minacce per Android si accresce molto velocemente in correlazione all'aumento del numero di dispositivi in uso.
- Già esistono trojan bancari per il SO Android.

- Dispositivi mobili potrebbero essere smarriti/rubati. Di conseguenza, le informazioni contenute su di essi (compresi username e password di accesso alle risorse aziendali) potrebbero arrivare nelle mani di persone poco amichevoli.

Soluzione

Il pacchetto di tariffa Dr.Web Premium include un abbonamento gratuito al programma Dr.Web per Android che consiste nei seguenti componenti di protezione:

- **Antivirus** – protegge il dispositivo da file malevoli, anche da quelli progettati per seguire gli spostamenti del proprietario del dispositivo e per intercettare le sue telefonate, conversazioni e messaggi.
- **Antifurto** – è un sistema di protezione contro i furti dei cellulari. Se il dispositivo è stato rubato o smarrito, è possibile cancellarne tutte le informazioni su remoto.
- **Antispam** – permette di proteggersi da chiamate ed SMS che non si vogliono ricevere e dai trojan che mandano messaggini a numeri ad elevato costo.

Da notare!

Tramite il Pannello di controllo del servizio "Antivirus Dr.Web", si può controllare in modo centralizzato il sistema di protezione antivirale su qualsiasi numero di dispositivi mobili Android (cominciando dalla versione 6.2).

Aggiornare regolarmente i database virali e i moduli del software

Minaccia

Un antivirus che non riceve aggiornamenti perché disabilitati dall'utente o che si aggiorna molto di rado non è capace di assicurare una protezione valevole.

Fatti

- I database virali Dr.Web si aggiornano più volte al giorno.
- Ogni giorno Doctor Web inserisce nei database circa duecento nuove definizioni che permettono di riconoscere la maggior parte di nuove minacce pervenuta per l'analisi.
- Gli aggiornamenti "caldi" si rilasciano appena una nuova minaccia sia stata analizzata.
- Prima di rilasciare gli aggiornamenti, essi vengono testati su un grande numero di file puliti - una procedura che permette di evitare falsi positivi.
- Gli aggiornamenti arrivano agli utenti da più server locati in diversi punti del globo terrestre.

Best practice

- Per mantenere **attuale** e **integro** il sistema di protezione antivirale, è necessario installare **tempestivamente** tutti gli aggiornamenti dei database virali e dei moduli dell'antivirus.
- Si deve TRASCURARE l'opinione del dipendente che non vuole riavviare il computer dopo un aggiornamento dell'antivirus.
- Solo una gestione **centralizzata** è in grado di assicurare aggiornamenti regolari e uno stato attuale dei componenti del sistema di protezione antivirale.
- Si deve controllare OGNI GIORNO se gli aggiornamenti si installino in modo normale perché non si può escludere la possibilità che appaiano virus capaci di disattivare aggiornamenti o di impedire l'accesso al server di aggiornamenti.

Attenzione!

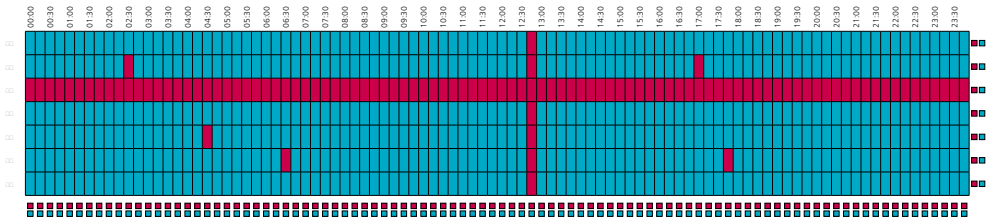
Nessun altro software richiede aggiornamenti tanto frequenti, quanto un antivirus. Nuovi virus emergono di continuo, perciò i database di firme antivirali devono essere aggiornati spessissimo.

Non disattivate mai la funzione di aggiornamento automatico dell'antivirus!

Soluzione

Il Pannello di controllo del servizio "Antivirus Dr.Web" è uno strumento per impostare con facilità gli aggiornamenti del sistema antivirale. Tramite questo software, si può proibire agli utenti di annullare aggiornamenti sulle postazioni protette. Si può scollegare dalla rete un agent non aggiornato e quindi prevenire l'eventuale propagazione di un malware dentro e al di fuori della rete. Inoltre è possibile:

- aggiornare i moduli Dr.Web sulle postazioni protette distribuendo il carico per diversi periodi;



- controllare lo stato dei database virali e delle postazioni;
- estendere le impostazioni di aggiornamento di una postazione verso un'altra oppure verso un gruppo (gruppi) delle postazioni.

Aggiornamento degli agent mobile

Rischio

Se nella rete locale vi è un computer protetto da un antivirus che si usa in maniera legittima, ma non si aggiorna ogni volta quando si rilasciano gli aggiornamenti, tale computer rappresenta un potenziale pericolo per l'intera rete locale. Non è da escludere che su tale computer potrebbe essere installato un sistema di home banking ...

Soluzione

Se un notebook sarà lontano dalla rete locale per un lungo tempo, l'agent antivirale può essere cambiato nella modalità mobile. La modalità mobile dell'agent disponibile nel servizio "Antivirus Dr.Web" consente all'agent di connettersi al server di aggiornamenti e ottenere gli update attuali anche quando il computer si trova fuori dalla rete aziendale. Questa possibilità è soprattutto utile in caso di viaggi di lavoro.

Obiettivo №5

Scansione delle postazioni a cadenze regolari

Rischi

- Un antivirus non conosce mai il 100% dei virus.
- Tra la comparsa di un virus nuovo e l'inserimento della definizione relativa nella base di dati potrebbero passare alcuni giorni e persino alcuni mesi.
- Anche se una definizione inserita nella base di dati può rilevare il virus relativo, ciò non significa che essa sarà in grado anche di curare questo virus – l'invenzione della cura opportuna potrebbe impiegare un lungo tempo.

Fatti

- La scansione successiva a un aggiornamento potrebbe rilevare sul computer parecchi programmi malevoli che prima l'antivirus non conosceva.
- Lo scanner antivirale esegue un controllo molto più profondo di quello che il file monitor esegue in background. È la causa perché qualche volta lo scanner scopre un virus che il file monitor non ha notato.

The best practice

- La scansione si deve eseguire almeno una volta alla settimana.
- Anche la cartella di quarantena si deve controllare regolarmente perché essa potrebbe contenere virus non conosciuti in precedenza o file spostati in seguito a un falso positivo.
- Nell'ambito aziendale, Va TRASCURATA l'opinione dell'utente su quanto spesso si devono eseguire le scansioni regolari.

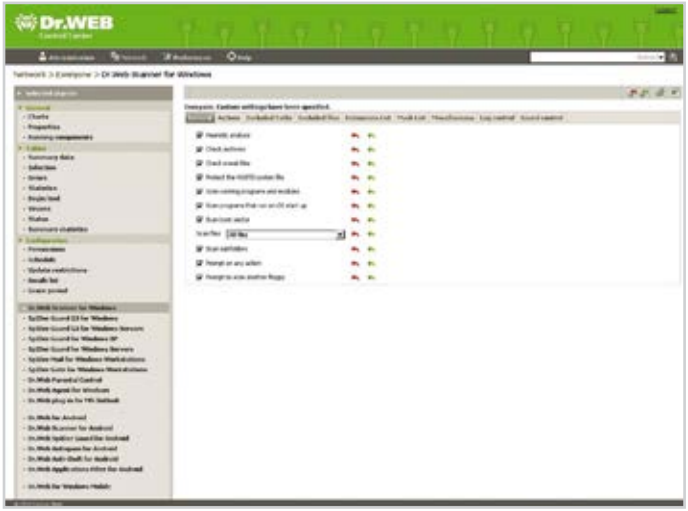
Soluzione

Le scansioni regolari di una postazione si impostano nello Scheduler il quale permette di:

- avviare le scansioni senza intervento da parte dell'utente della postazione;
- stabilire qualsiasi cadenza delle scansioni, perciò è possibile eseguire le scansioni in un tempo conveniente per i dipendenti;
- lanciare una scansione obbligatoria con partenza del computer;
- definire percorsi (aree, dischi e cartelle da controllare necessariamente) e anche esclusioni;
- impostare una sequenza di azioni automatiche da applicare ai file malevoli e sospetti rilevati dallo scanner.

Attenzione!

Gli sviluppatori di Dr.Web hanno già assegnato i parametri migliori di scansione nelle impostazioni predefinite. Si consiglia di non modificarli senza una reale necessità.



Controllare in modo centralizzato come si eseguono le scansioni regolari delle postazioni

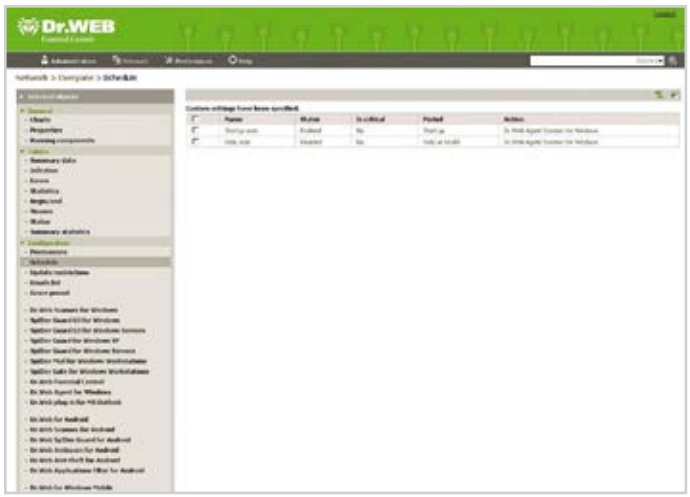
Best practice

- L'unica possibilità di eseguire sempre le scansioni regolari su tutte le postazioni è **proibire in modo centralizzato** a tutte le postazioni di disattivare la scansione.

Soluzione

Il Pannello di controllo del servizio "Antivirus Dr.Web" permette di eseguire scansioni regolari e di osservare le relative politiche di sicurezza. Tramite Pannello di controllo si possono compiere le seguenti azioni:

- avviare/terminare scansioni senza intervento da parte dell'utente della postazione;
- impostare percorsi di scansione;
- stabilire calendari di scansione per singole postazioni e per gruppi, cioè eseguire le scansioni in qualunque tempo sia conveniente per i dipendenti.



Inoltre il Pannello di controllo consente di avviare/terminare ogni modulo dell'agent antivirale (eccetto SpIDer Guard).

Obiettivo №7

Limitazione di accesso a supporti rimovibili

Attenzione!

Queste funzioni sono disponibili solo nel pacchetto di tariffa Dr.Web Premium.

Minaccia

- Ogni giorno emergono tantissimi virus e l'antivirus non può conoscerne tutti – quindi esiste sempre il rischio che il computer si infetti da un malware sconosciuto.
- Persino nei sistemi d'informazione altamente protetti, virus si propagano non dalle email, ma dai supporti rimovibili (perlopiù chiavette USB) che quindi sono la fonte maggiore di infezione.

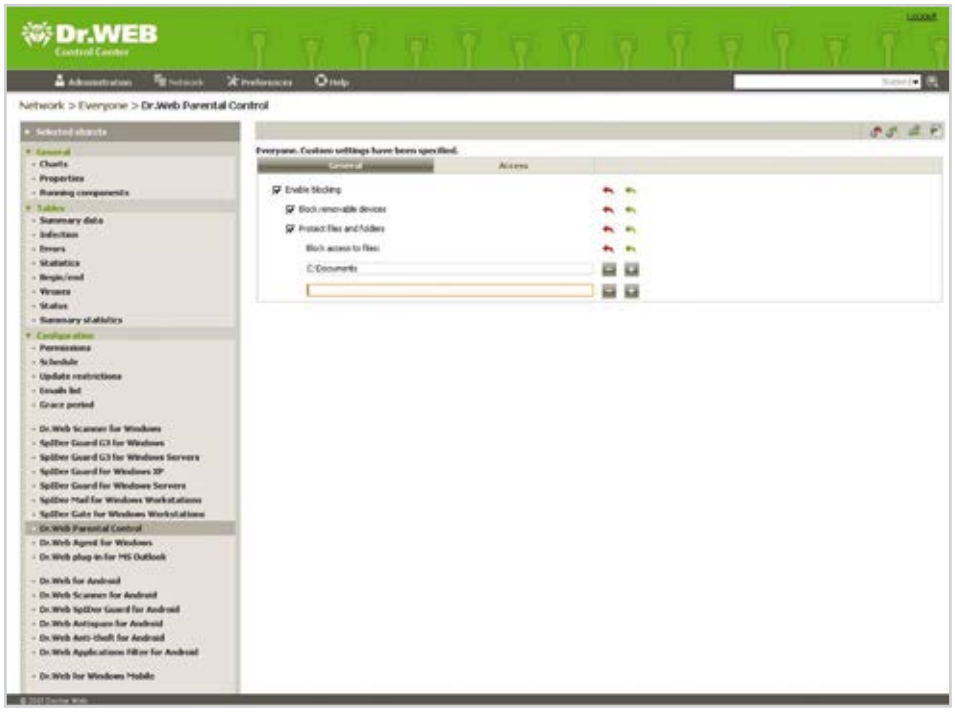
Attenzione!

Supporti rimovibili sono non solo flash drive, ma **qualsiasi periferica connessa al computer tramite una porta USB!** È possibile trapiantare un virus da un computer a un altro persino con una macchina fotografica o un lettore MP3.

- La maggior parte di minacce moderne è categorizzata come cavalli di troia. I trojan sono programmi interamente malevoli che non possiedono una funzione di proliferazione automatica e non possono propagarsi da soli. Senza saperlo, gli utenti portano i trojan da un computer a un altro su chiavette USB.
- Secondo le varie stime, i dati si perdono in seguito alle attività dei virus con un tasso dal 7% al 22% dei casi.
- Le conseguenze delle attività virali possono essere la perdita di informazioni importanti, la disconnessione dell'azienda da Internet, l'inattività per il tempo di ripristino dei computer infetti.
- Se nella rete locale persiste il rischio di infezione, ciò distrae gli amministratori di sistema da altri compiti necessari per il progresso dell'impresa.

Soluzione

Per proibire completamente di usare supporti rimovibili sulle postazioni, abilitate l'opzione "Bloccare supporti rimovibili" nelle impostazioni del modulo Office Control di Dr.Web. Così si ostacola una delle vie principali (supporti rimovibili) da cui virus penetrano nella rete locale.



L'Office Control di Dr.Web offre le seguenti possibilità:

- determina i file e le cartelle della rete locale a cui il dipendente può accedere e impedisce l'accesso a quelli che devono restare non accessibili. Così l'Office Control consente di proteggere le informazioni importanti da un danneggiamento o una rimozione intenzionale o casuale e dal furto delle informazioni da parte dei malintenzionati o dei dipendenti stessi (quelli che vogliono sfruttare le informazioni riservate ai fini personali);
- limita o proibisce del tutto l'accesso a risorse di Internet e a supporti rimovibili, dunque esclude l'eventualità che i virus penetrino attraverso questi percorsi.

Vi è un modo addizionale di come si può impedire ai virus di entrare sul computer dai supporti rimovibili. Il file monitor SpIDer Guard ha una funzione che proibisce l'esecuzione automatica di programmi da supporti rimovibili. Se è abilitata l'opzione "Bloccare avvio automatico da supporti rimovibili", si può continuare a usare i dischi di memoria flash nei casi in cui non è possibile farne di meno.

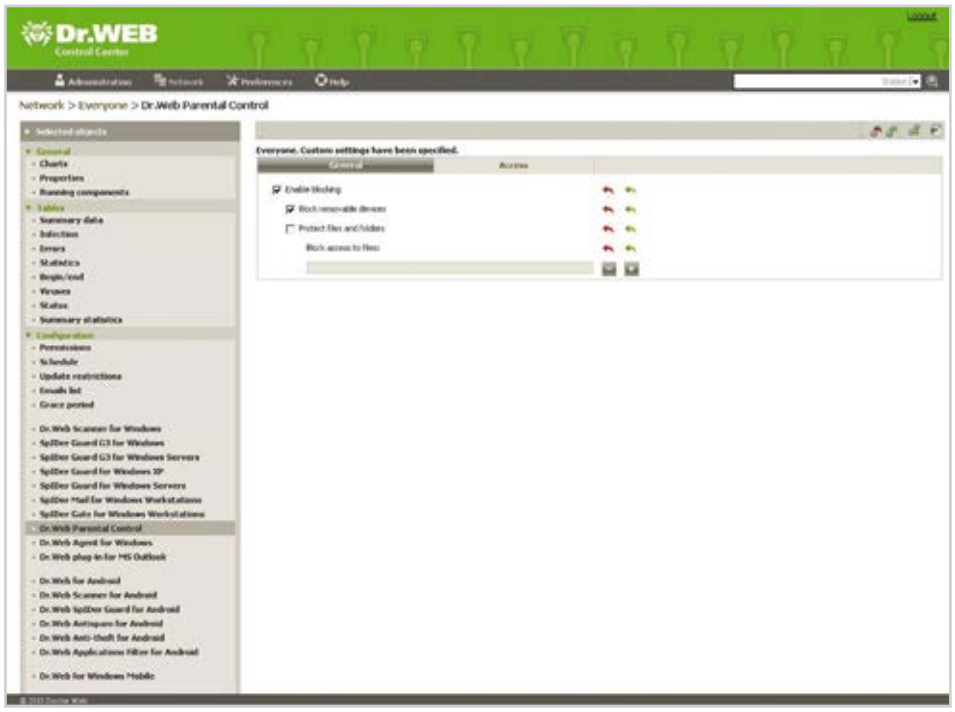
Le azioni sopranominate sono efficaci, ma non sufficienti perché le impostazioni relative possono essere trovate e disattivate dal dipendente.

Best practice

L'utente o un malware avviato in suo nome non devono avere accesso a nessuna risorsa locale o di rete, salvo quelle che sono necessarie per adempiere i compiti di lavoro. È inutile cercare di convincere il personale che le chiavette USB potrebbero rappresentare una minaccia. È molto più semplice **impedire in modo centralizzato l'accesso** a queste periferiche.

Soluzione

Il **divieto centralizzato** di usare supporti rimovibili si configura nel Pannello di controllo del servizio "Antivirus Dr.Web".



Obiettivo №8

Limitazione di accesso a siti web

Proteggersi da programmi malevoli e da phishing

Minaccia

Durante il lavoro, i dipendenti leggono notizie per essere al corrente. Il rischio qui è che la maggior parte dei dipendenti:

- accede a Internet dal computer di ufficio;
- usa Windows con i permessi di amministratore;
- usa password semplicissime e facili da indovinare;
- non installa gli aggiornamenti di sicurezza per tutti i software usati sul PC.

La navigazione libera dei dipendenti potrebbe comportare l'eventuale fuga di informazioni o la sostituzione o rovina dei documenti importanti.

Quali siti web sono le più frequenti fonti di malware e di attacchi phishing (in ordine decrescente di frequenza di incidenti)?

- Siti di tecnologia e telecomunicazione.
- Siti concernenti l'impresa: giornali e notizie di business, siti e forum della contabilità, corsi di formazione online, servizi concepiti per aumentare l'efficacia aziendale.
- Siti pornografici.

Best practice

Il sistema di protezione antivirale deve controllare ogni collegamento al download dal web e l'intero traffico prima del suo arrivo sul computer.

Soluzione

Per proteggersi da virus durante le visite su un sito compromesso, si consiglia di usare la protezione integrata.

Da notare!

Tramite le funzioni del sistema di protezione antivirale Dr.Web è possibile:

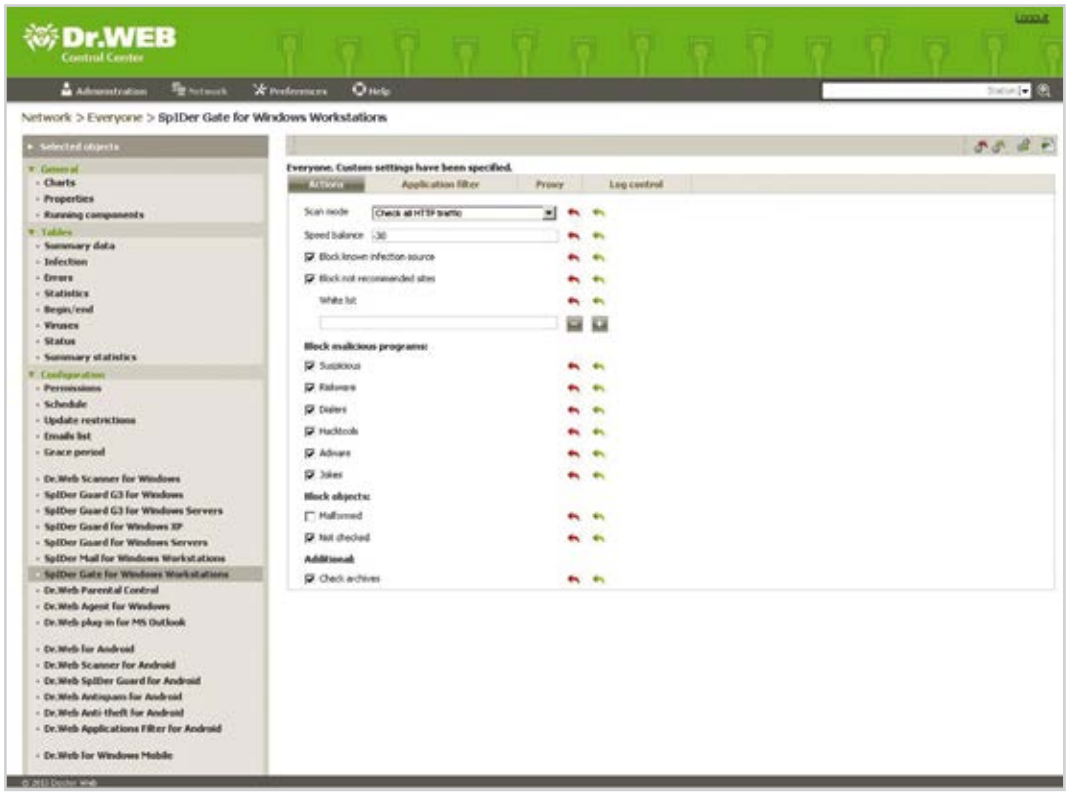
- limitare parzialmente l'accesso a Internet;
- tenere white list e black list di indirizzi per non dover impedire completamente l'accesso a Internet per un dipendente che deve usare la rete ai fini di lavoro;
- prendere delle precauzioni bloccando completamente l'accesso a Internet (per esempio, sulle postazioni nel reparto contabilità);
- assicurare che gli utenti non possano disattivare queste restrizioni dalle postazioni.

Capacità di protezione del nucleo antivirale di Dr.Web

- **Tecnologia ScriptHeuristic** – impedisce l'esecuzione di qualsiasi script dannoso nel browser e in documenti PDF, senza compromettere la funzionalità di script legittimi.
- **Individuazione di minacce nuove con un'analisi euristica** – serve per rilevare virus nuovi, non conosciuti prima e non inclusi nella base di dati dell'antivirus.
- **Tecnologia Fly-Code** – rileva virus conosciuti nascosti da packer sconosciuti.
- **Sottosistema di scansione e di neutralizzazione in background di minacce attive, parte del componente Antirootkit Dr.Web (Anti-rootkit API, arkapi)** – il sottosistema risiede nella memoria e cerca minacce attive nelle aree critiche di Windows, quali oggetti in avvio automatico, processi e moduli in esecuzione, l'euristica di modifiche in oggetti di sistema, la memoria operativa, i MBR/VBR dei dischi, nonché il BIOS del computer. Rilevata una minaccia, il sottosistema cura il computer e blocca effetti dannosi.

Capacità di protezione dei componenti antivirali installati sulle postazioni

- **File monitor SplDer Guard** – protegge dalle infezioni attive nel sistema.
- **Dr.Web Office Control** – confronta indirizzi dei siti con la base di dati attuale dei siti pericolosi e sconsigliati in dieci categorie (social network, giochi d'azzardo ecc.).
- **Monitoraggio HTTP SplDer Gate®** – esegue un controllo sulla base delle firme antivirali e un controllo con i metodi euristici e scansiona il traffico prima della sua entrata nel browser.
- Il modulo SplDer Gate scansiona in tempo reale e in modo trasparente il traffico HTTP in entrata, intercetta tutte le connessioni HTTP/HTTPS, filtra dati, blocca automaticamente pagine infette in qualunque browser, controlla file compressi in archivi (per esempio, file scaricati tramite il download manager e molte altre applicazioni che scambiano dati con web server), protegge da siti di phishing e da altri siti pericolosi.
- È possibile disattivare il controllo del traffico in uscita o in entrata, nonché si può creare una lista delle applicazioni, il cui traffico HTTP verrà controllato in ogni caso e per l'intero (black list). Inoltre è possibile escludere dal controllo il traffico di alcune applicazioni (white list).
- Il funzionamento di SplDer Gate non dipende dal browser in uso.
- Il filtraggio non ha quasi nessun effetto sulle prestazioni del computer, sulla velocità del lavoro in Internet e sulla quantità di dati trasmessi.
- Con le impostazioni predefinite, non è necessario configurare il modulo perché SplDer Gate inizia la scansione subito dopo l'installazione.



Attenzione!

Questi moduli sono disponibili solo nel pacchetto di tariffa Dr.Web Premium.

Obiettivo №9

Risparmiare sulle spese di traffico e controllare le attività dei dipendenti

Rischio

- Se ciascun dipendente usa Internet ai fini personali solo per un'ora al giorno, i costi ammontano al 12,5 % degli stipendi pagati dall'azienda.
- In alcuni periodi del giorno lavorativo (per esempio, nella pausa di pranzo) i dipendenti occupano fino all'80 % della larghezza di banda per le attività non legate al lavoro.

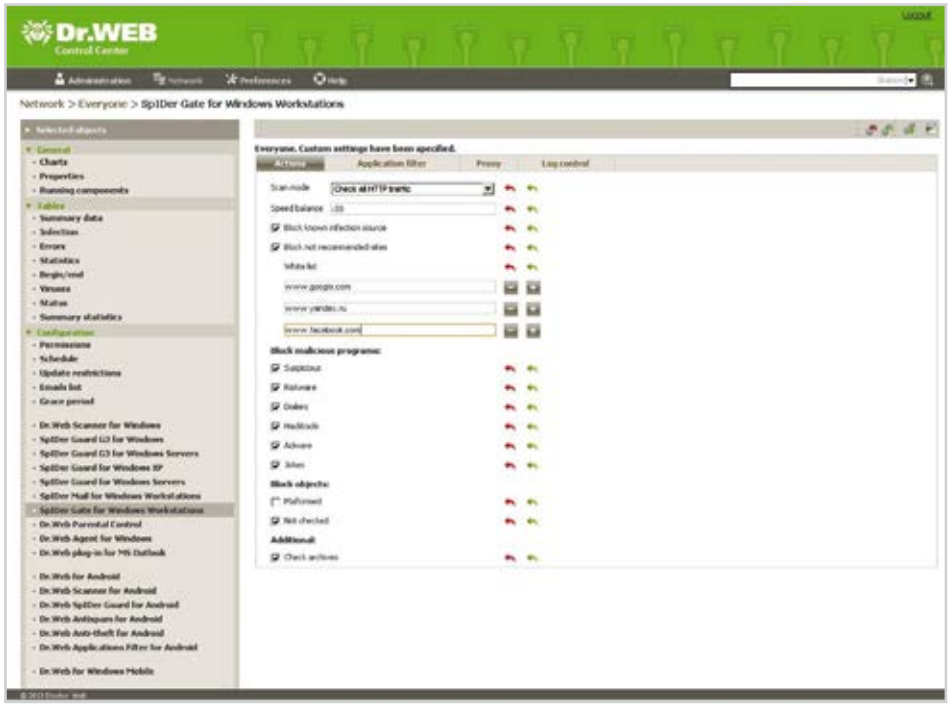
Best practice

- Nelle ore lavorative, il personale deve avere accesso solamente alle risorse del web che sono necessarie per lo svolgimento delle attività lavorative.
- Si può imporre **un divieto centralizzato** e impedire l'accesso del personale alle risorse del web non ritenute necessarie.
- NON SI DEVE PRENDERE IN CONSIDERAZIONE l'opinione dei dipendenti riguardante il carattere dei siti web (se siano sicuri o meno).

Soluzione

La gestione centralizzata disponibile nel servizio "Antivirus Dr.Web" consente di:

- determinare le politiche di accesso a risorse di Internet per gruppi di utenti o per singoli utenti;
- impedire agli utenti di visitare siti web indesiderati, per esempio, social network, negozi elettronici, siti di gioco.



Protezione contro lo spam

Attenzione!

Queste funzioni sono disponibili solo nel pacchetto di tariffa Dr.Web Premium.

Ridurre il traffico occupato da email indesiderate e allontanare quasi tutte le minacce trasmesse nello spam

Rischi

1. Il traffico di email è **il veicolo principale** di propagazione dei virus e dello spam. Se il computer si infetta, i programmi malevoli potrebbero accedere alla rubrica dell'utente che potrebbe contenere gli indirizzi email dei colleghi, partner e clienti, così il malware comincia a diffondersi non solo dentro la rete locale, ma anche fuori.
2. I dipendenti spesso ignorano le nozioni di sicurezza informatica o non sono abbastanza attenti nell'uso del computer. Di conseguenza i computer aziendali potrebbero diventare parte di una botnet e all'insaputa degli utenti potrebbero inviare email in grande quantità. Tale circostanza potrebbe danneggiare la buona fama dell'azienda. L'azienda potrebbe essere inserita nelle black list e la sua connettività a Internet potrebbe essere bloccata.

Rischi dell'uso dell'antivirus senza antispam

Rischi causati dai virus	Rischi di reputazione
▪ Un computer infettato potrebbe diventare parte di una botnet e potrebbe subire un attacco, compresi attacchi DoS. ▪ L'azienda potrebbe essere compromessa: i suoi indirizzi vengono aggiunti alle black list e la sua connettività a Internet si toglie perché i suoi computer, diventati bot, inviano messaggi indesiderati in grande quantità. ▪ Aumento dei costi informatici (pagamento per il traffico superfluo occupato dallo spam / costi di memorizzazione di email fra le quali anche email di spam), aumento delle spese per il traffico.	▪ I partner e clienti non ricevono le email dall'azienda perché essa è stata inserita nelle black list. ▪ I partner e clienti ritengono che la reputazione dell'azienda sia peggiorata. ▪ Si forma un'opinione che l'azienda usi tecnologie superate. ▪ I clienti rinunciano ai servizi dell'azienda.

Opinione sbagliata

L'antispam necessita di un training continuo.

Fatti

A differenza degli antispam che richiedono training e a cui l'amministratore di sistema deve prestare un'attenzione quotidiana, il sistema intellettuale di filtraggio spam Dr.Web non necessita di essere impostato o addestrato.

Best practice

- Il traffico di email deve essere scansionato prima dell'arrivo di una lettera nel programma di email. Ciò si fa per evitare che il codice dannoso sfrutti le vulnerabilità del programma di email.
- Il traffico di email può essere protetto validamente solo da soluzioni integrate che combinano un antivirus e un antispam. Inoltre, tali soluzioni permettono di ridurre le spese improduttive, cioè perdite causate da mancata organizzazione e gestione della produzione.

Soluzione

L'antispam Dr.Web, parte del file monitor SpIDer Mail, scansiona le email prima che pervengano nel client di email e impedisce che i malware, contenuti nello spam, sfruttino le vulnerabilità del software. L'antispam non rallenta le prestazioni del sistema e l'efficacia di filtraggio spam raggiunge il 97–99%.

Obiettivo №11

Vantaggi dell'antispam Dr.Web

- **L'antispam Dr.Web non necessita del training** – a differenza degli antispam che richiedono training e cui l'amministratore di sistema deve prestare un'attenzione quotidiana, il sistema intellettuale di filtraggio spam Dr.Web non necessita di un'impostazione dei parametri e comincia a filtrare lo spam automaticamente con la ricezione della prima email.
- **Filtraggio efficace dello spam** – il componente include svariate tecnologie di filtraggio che permettono di riconoscere con un elevato grado di probabilità email del genere spam, phishing, pharming, scamming e bounce (risposta tecnica di mancata consegna).
- **Protegge il computer dall'inserimento nelle botnet** – il Vostro ISP non disconnetterà la Vostra azienda da Internet per la diffusione dello spam.
- **Le email non si perdono** – le email bloccate dall'antispam non vengono rimosse, ma messe in una cartella speciale del client di posta (se tale cartella è impostata sulla postazione locale). Tali email possono essere scorse per assicurarsi che non vi siano stati falsi positivi.
- **Risparmio del traffico** – il modulo analizzatore spam è assolutamente autonomo; non necessita della connessione a un server esterno o dell'accesso a qualche base di dati.
- **Sempre attuale** – le tecnologie uniche di individuazione di email indesiderate includono più migliaia di regole perciò gli aggiornamenti non devono essere frequenti e possono essere eseguiti una volta al giorno.
- **Non impone un peso percettibile sul sistema** – l'antispam non rallenta le prestazioni del sistema e non aumenta il tempo necessario per ricevere le email.

Incrementare il rendimento dei dipendenti

Quando esiste un eccesso di produzione delle informazioni, l'attenzione delle persone diventa una risorsa preziosa e quasi non rinnovabile. Con la venuta di Internet, i dipendenti affrontano al posto di lavoro un grande flusso e persino un eccesso delle informazioni. La loro attenzione si disperde se devono ripulire le caselle postali da messaggi indesiderati o chiudere continuamente finestre pop-up e banner promozionali. Tali fattori abbassano il livello di concentrazione e hanno un impatto negativo sulle condizioni emotive e psichiche delle persone. Di conseguenza, è negli interessi dell'azienda eliminare i fattori che distraggono l'attenzione dei dipendenti.

Rischi

1. Un dipendente spende in media da 6 a 11 minuti al giorno scorrendo e rimuovendo messaggi indesiderati.
2. La più alta è la responsabilità di un dipendente, il più perde l'azienda quando gli paga per un tempo non impiegato nel lavoro.

Rischi

Si usa solo antivirus senza antispam:

- si abbassa il rendimento di tutti i dipendenti che ricevono email e devono occuparsi della pulitura della casella postale dallo spam;
- perdite di tempo lavorativo – i dipendenti compiono le loro funzioni in ritardo e quindi l'azienda non può adempiere tempestivamente i suoi obblighi nei confronti dei clienti e partner;
- la sovrabbondanza delle informazioni disperde l'attenzione e aumenta la stanchezza;
- se i dirigenti dell'azienda non possono risolvere il problema, il personale rimane deluso (un alto rischio di reputazione!).

Soluzione

L'antispam incluso nel pacchetto Dr.Web Premium è uno strumento efficace per affrontare molteplici fattori distraenti. L'antispam Dr.Web permette di ridurre le perdite di tempo lavorativo perché:

- il computer può funzionare in modo normale e sicuro (niente virus o spam nel traffico di email);
- le caselle postali dei dipendenti non contengono messaggi indesiderati e i dipendenti non devono distrarsi dal lavoro per ripulirle.

Configurare il filtraggio dello spam su una postazione

L'antispam viene abilitato nel componente Dr.Web SpIDer Mail.

Black list e white list

Se è necessario, si possono creare liste degli indirizzi affidabili o proibiti, e le email arrivate da tali indirizzi verranno filtrate automaticamente in modo desiderato.

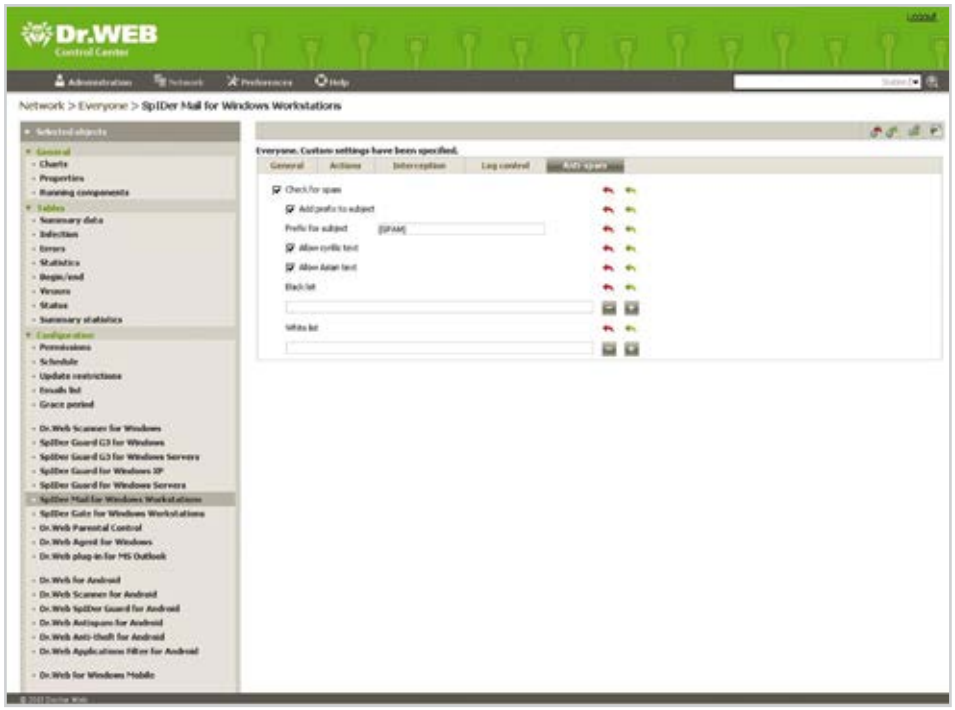
Controllo centralizzato per impedire la disattivazione dell'antispam

Best practice

L'unico modo efficace per impedire ai dipendenti di disattivare l'antispam o di modificare le white list e le black list è un divieto centralizzato che blocca l'accesso alle impostazioni dell'antispam.

Soluzione

La configurazione centralizzata dell'antispam è disponibile nel Pannello di controllo del servizio "Antivirus Dr.Web".



Obiettivo №13

Protezione contro gli attacchi di virus su dispositivi con sistemi di home banking

Vi ricordiamo!

1. Le minacce informatiche moderne vengono create da gruppi criminali ai fini di rubare soldi dalle persone private e dalle aziende.
2. Vulnerabilità sono presenti in ogni software, anche nei sistemi di home banking.

Metodi di attacchi mirati al furto di denaro

I virus possono infiltrarsi o possono essere inseriti deliberatamente su un dispositivo su cui si usa un sistema di home banking tramite i seguenti metodi:

- Siti di phishing
- Creazione dei siti fraudolenti
- Violazione dei siti e delle risorse web popolari
- Metodi di social engineering
- Violazione dei computer

Tipi di attacchi mirati al furto di denaro

- Il computer si infetta tramite un web inject (talvolta con il reindirizzamento a un sito di phishing).
- I canali di trasferimento dati vengono attaccati. Per ricavare il login e la password, vengono intercettate le query http o le informazioni dai moduli visualizzati sullo schermo.
- I server vengono attaccati dai virus. Tale attacco potrebbe essere finalizzato a trovare vulnerabilità sul server del sistema di home banking oppure a nascondere furti del denaro.
- Il computer viene attaccato da Internet per rubare la chiave segreta di firma elettronica, nonché le password.
- Il computer viene attaccato da Internet per stabilire il controllo remoto sulle risorse del calcolo locali.
- Si esegue un attacco ai fini di sostituire un documento prima che venga firmato.
- Si esegue un attacco ai fini di sostituire parzialmente o completamente il software in uso sul computer.
- Nel software si incorporano backdoor o cavalli di troia.

Quali dispositivi sono sotto attacco

- postazioni d'ufficio;
- dispositivi personali dei dipendenti dell'azienda attaccata;
- dispositivi personali dei clienti dell'azienda attaccata.

Obiettivi degli attacchi

- rubare o sostituire le credenziali di autenticazione (login, password) per accedere al sistema di home banking;
- effettuare transazioni bancarie accedendo su remoto in una sessione esistente o parallela;
- penetrare nella rete protetta dell'azienda.

Metodi di furto

- I criminali creano un ordine di pagamento falso direttamente sul computer remoto utilizzando programmi malevoli.
- I criminali inviano un ordine di pagamento falso tramite il computer remoto su cui è aperta una sessione di home banking (è possibile firmare il documento falso con la chiave custodita su un supporto separato, per esempio, eToken, iKey ecc.).

Un cliente indignato:

"Abbiamo comprato un antivirus. L'amministratore di sistema lavora sodo. I sistemi si aggiornano ... Tuttavia i soldi sono stati rubati! Di chi è la colpa?"

Fatti

1. In moltissime aziende medie e piccole, solo il direttore amministrativo è autorizzato a firmare gli ordini di pagamento, sebbene due firme digitali, quella del direttore e quella del ragioniere, possano proteggere meglio le transazioni finanziarie dell'azienda.
2. I dipendenti accedono al sistema di home banking non solo dalle postazioni di ufficio, ma anche dai computer casalinghi e dai dispositivi mobili (comunemente Android) i quali spessissimo non dispongono di alcun antivirus o ne hanno una versione gratuita a funzioni ridotte.

Non esistono informazioni statistiche unificate che si riferiscono ai furti di denaro in sistemi di home banking tramite l'utilizzo di programmi malevoli. Spesso le persone interessate non si rivolgono alla polizia pensando che non sia possibile recuperare i fondi rubati. Le vittime non sanno come comportarsi in una situazione di emergenza e non conoscono la procedura con la quale si può aprire un'inchiesta, così perdono tanto tempo prezioso.

Rischi

1. I trojan moderni hanno lo scopo di rubare soldi da aziende e persone private.
2. Il trojan bancario Carberp – il più pericoloso – si propaga utilizzando Black Hole Exploit Kit, cioè una raccolta di exploit che sfruttano falle e funzioni non documentate dei programmi moderni, in particolare, dei browser e dei sistemi operativi.
3. Il trojan Carberp viene sviluppato e commercializzato da un gruppo criminale organizzato. Gli sviluppatori lavorano in un paese, i server da cui si diffonde il trojan sono locati in un altro paese, gli organizzatori agiscono da un altro paese ancora, mentre i "partner", cioè criminali che comprano una parte della botnet per svolgere attività illecite, si trovano in più paesi.
4. Il cavallo di troia può scaricare plugin speciali. Attualmente esistono le versioni dei plugin per la maggior parte dei sistemi di home banking. Tra i comandi che il trojan Carberp può eseguire, sono i seguenti: lanciare qualsiasi file sul computer infetto, aprire una sessione del desktop remoto tramite il protocollo RDP e persino eliminare il sistema operativo dal PC infetto. Con il controllo remoto e i plugin speciali, è possibile organizzare un attacco "su misura", cioè i cybercriminali possono determinare le azioni che il trojan deve eseguire sui computer di una concreta società.
5. I virus dalla famiglia Carberp penetrano sul computer mentre l'utente visita siti web violati, fra cui siti di notizie e di contabilità visitati giornalmente. Non è necessaria un'azione da parte dell'utente per far passare il virus perché l'infezione avviene automaticamente.
6. Al trojan bancario Carberp bastano da uno a tre minuti per rubare le password e il denaro dal conto della vittima.
7. Ogni giorno i database virali di Dr.Web vengono completati con più definizioni di questo trojan: si vede che il codice del cavallo di troia viene perfezionato continuamente dai suoi autori. Il seguente esempio mostra quanti record si aggiungono al database virale ogni giorno:

```
Trojan.Carberp.14(2) Trojan.Carberp.15(7) Trojan.Carberp.194 Trojan.Carberp.195
Trojan.Carberp.196 Trojan.Carberp.197 Trojan.Carberp.198 Trojan.Carberp.199 Trojan.Carberp.200
Trojan.Carberp.201 Trojan.Carberp.202 Trojan.Carberp.203 Trojan.Carberp.204 Trojan.Carberp.205
Trojan.Carberp.206 Trojan.Carberp.207 Trojan.Carberp.208(14) Trojan.Carberp.209
Trojan.Carberp.210 Trojan.Carberp.211 Trojan.Carberp.212 Trojan.Carberp.214 Trojan.Carberp.215
Trojan.Carberp.216 Trojan.Carberp.217 Trojan.Carberp.218 Trojan.Carberp.219 Trojan.Carberp.220
Trojan.Carberp.221 Trojan.Carberp.222 Trojan.Carberp.224 Trojan.Carberp.225 Trojan.Carberp.226
Trojan.Carberp.227 Trojan.Carberp.228 Trojan.Carberp.229 Trojan.Carberp.230 Trojan.Carberp.231
Trojan.Carberp.232 Trojan.Carberp.233 Trojan.Carberp.234 Trojan.Carberp.235 Trojan.Carberp.236
Trojan.Carberp.237 Trojan.Carberp.238 Trojan.Carberp.239 Trojan.Carberp.240 Trojan.Carberp.241
Trojan.Carberp.242 Trojan.Carberp.243Trojan.Carberp.244 Trojan.Carberp.245 Trojan.Carberp.246
Trojan.Carberp.247 Trojan.Carberp.248 Trojan.Carberp.249 Trojan.Carberp.250 Trojan.Carberp.251
Trojan.Carberp.252 Trojan.Carberp.253 Trojan.Carberp.254 Trojan.Carberp.255 Trojan.Carberp.256
Trojan.Carberp.257 Trojan.Carberp.258 Trojan.Carberp.259 Trojan.Carberp.260 Trojan.Carberp.261
Trojan.Carberp.262 Trojan.Carberp.263 Trojan.Carberp.264 Trojan.Carberp.265 Trojan.Carberp.266
Trojan.Carberp.267 Trojan.Carberp.29(14) Trojan.Carberp.33(10) Trojan.Carberp.45(4)
Trojan.Carberp.5(3) Trojan.Carberp.60(6) Trojan.Carberp.61 Trojan.Carberp.80
```

   E questo è solo uno dei moltissimi cavalli di troia ...

Che può fare un'azienda per opporsi a questa minaccia se ha solo un file antivirus senza funzioni di protezione integrata? – NIENTE.

Best practice

1. Solo un antivirus non basta per difendere la rete aziendale contro le minacce moderne. Per ridurre il rischio di infezione, il sistema di protezione antivirale deve comprendere:
   - Un software progettato per curare infezioni attive – rende inattivi i programmi malevoli infiltratisi nella rete locale e ripulisce i computer da essi.
   - Una valida sistema di auto-protezione – con esso la rete locale può funzionare in modo normale fino a quando non arriveranno gli aggiornamenti dei database virali che permettono di curare le infezioni presenti.

- Office control — un modulo che può limitare l'accesso degli utenti ai siti web (va ricordato che i trojan si diffondono attraverso siti web).
- Un modulo di controllo dei collegamenti ipertestuali (monitoraggio HTTP).
- Pannello di controllo — rende possibile una gestione centralizzata, quindi i dipendenti non possono modificare le impostazioni di protezione con il pretesto che "il computer è lento".

2. La pratica dimostra che i dipendenti effettuano pagamenti non solo dalle postazioni di ufficio, ma anche dai computer casalinghi e dai dispositivi mobili. Di conseguenza, è necessario proteggere tutti i computer e dispositivi da cui lavorano i dipendenti dell'azienda.
3. Il computer aziendale su cui è installato un software di contabilità o di home banking deve essere completamente scollegato da Internet. Inoltre, con le impostazioni CENTRALIZZATE, è necessario impedire di utilizzare su di esso supporti rimovibili.*
4. Va IGNORATA l'opinione degli addetti alla contabilità riguardante i provvedimenti di protezione intrapresi su tale computer.

** È possibile impostare tale divieto tramite il componente Office control che fa parte del pacchetto di tariffa Dr.Web Premium.*

Fatti

Esiste già un trojan bancario studiato per la piattaforma mobile Android — il suo nome è Android.SpyEye.1.

Che fare se il denaro è stato rubato tramite il sistema di home banking

Spesso le vittime si accorgono troppo tardi del furto di denaro, quando il crimine è già stato compiuto. In questo momento, diventa molto importante un'adeguata reazione all'incidente. Prima del tutto, è necessario accertarsi che il furto sia stato causato da un virus informatico. Si deve interrogare il personale che ha accesso al sistema di home banking. Se nessuno di loro ha compiuto la transazione sospetta, ciò significa che molto probabilmente ha agito un virus o un criminale penetrato nel sistema.

Attenzione!

- Non cercate di aggiornare l'antivirus o lanciare la scansione — così si distruggono le tracce degli intrusi nel sistema!
- Non cercate di reinstallare il sistema operativo!
- Non cercate di rimuovere alcuni file o programmi dal disco!
- Non utilizzate il computer da cui si suppone che siano state rubate le informazioni di autenticazione del sistema di home banking — anche se l'uso di questo computer fosse essenziale!

Dovreste agire in modo veloce e decisivo:

1. Chiamate subito alla Vostra banca perché possibilmente il pagamento potrebbe essere fermato ancora. Anche se il denaro è già stato trasferito, chiedete di sospendere tutte le transazioni sul conto compromesso fino al rilascio dei nuovi mezzi di autenticazione (le credenziali di accesso, etoken ecc.).
2. Scrivete una dichiarazione alla Vostra banca (banca del mittente del pagamento) e la inviate per fax. Stampate la dichiarazione in TRE copie e le consegnate alla banca. Chiedete di mettere il numero di registrazione su due copie: una copia rimane nella Vostra azienda, mentre l'altra copia sarà allegata alla Vostra denuncia sporta alla polizia. Il dipendente della banca che ha accettato la Vostra dichiarazione deve metterci la data e il numero seriale del documento accettato.
3. Scrivete una dichiarazione alla banca del beneficiario del pagamento effettuato dal Vostro conto e la inviate per fax. Stampate TRE copie della dichiarazione e le fate registrare dalla banca del beneficiario ugualmente di come abbiamo descritto nel punto precedente.
4. Sporgete una denuncia alla polizia con le due dichiarazioni allegate (quelle consegnate alla banca del mittente del pagamento e alla banca del beneficiario).
5. Scrivete una richiesta al Vostro ISP in cui chiedete di mandarVi i log di connessioni alla rete nel periodo quando è stato compiuto il furto.

Attenzione!

Gli ISP conservano i log di connessioni alla rete per due giorni al massimo — quindi avete poco tempo per agire!

Tutto ciò deve essere fatto entro uno o due giorni dal momento quando avete scoperto il furto!

Protezione da attacchi di hacker

Tipi di attacchi di hacker

Esistono moltissimi tipi di attacchi alla rete. Di solito, i malintenzionati sfruttano le vulnerabilità del sistema operativo o di altro software installato sul computer assalito o le sue limitazioni di risorse del calcolo. I tipi di attacchi più diffusi sono i seguenti:

- Gli attacchi DoS o DDoS (comportano la negazione di un servizio) sono intesi a mettere temporaneamente fuori servizio il sistema sotto mira.
- Gli attacchi di password sono ideati per scoprire le password in uso tramite il metodo a forza bruta o il metodo di social ingeneering.
- Lo Spoofing è un metodo che inserisce informazioni false o comandi dannosi nel flusso di dati normale, reindirizza il traffico a un indirizzo IP fraudolento o sostituisce l'indirizzo IP.
- Con lo Sniffing si intercetta il traffico (per esempio tutte le email della vittima) per la successiva analisi.
- Dirottamento della sessione TCP (TCP Session Hijacking).
- Man-in-the-Middle. L'attaccante si trova tra due host della rete e, infatti, agisce come un server proxy, controllando le informazioni trasmesse e modificandole ai propri scopi. Gli obiettivi di tali attacchi sono: rubare informazioni, intercettare la sessione corrente e accedere alle risorse di rete private, analizzare il traffico e ottenere informazioni sulla rete e sui suoi utenti, effettuare attacchi del tipo DoS, distorcere i dati trasmessi e inserire informazioni non autorizzate in sessioni di rete.

Non è tutto. Come attacchi di rete, possono essere categorizzati tutti i metodi di spionaggio tramite la rete, di abuso di fiducia e di accesso non autorizzato. Per esempio, vediamo il port scanning (scansione delle porte): questo tipo di minaccia non è un attacco, ma di solito precede a un attacco essendo uno dei metodi principali per ricavare informazioni sull'host remoto. Le informazioni ottenute dalla scansione (uno "snapshot" del sistema) permettono al cybercriminale di identificare il tipo di sistema operativo installato sul computer remoto e così anche le sue vulnerabilità tipiche.

Emergono di continuo nuovi tipi di attacco. In particolare, quando aziende hanno cominciato a usare il cloud computing, i canali di trasferimento dati sono stati attaccati con maggiore intensità. Insieme con l'introduzione del protocollo IPv6 sono stati pensati nuovi tipi di attacco che si basano sulle vulnerabilità di questo protocollo la cui attuazione è ancora in fase di perfezionamento.

Conseguenze degli attacchi

- Danneggiamento o distruzione delle risorse d'informazione, impossibilità di usarle che comporta l'inattività lavorativa.
- Furti dei dati riservati, comprese password, email e qualsiasi informazione che può essere rubata.
- Rischi reputazionali, per esempio il ritardo o l'impossibilità di adempimento degli obblighi riguardo ai clienti e partner.

Attenzione!

Di solito, gli attacchi finalizzati all'introduzione del software dannoso passano inosservati dalle vittime i cui computer cadono sotto il controllo dei malintenzionati.

Obiettivi degli attacchi

- Motivi di politica.
- Azioni dei concorrenti (compresi spionaggio industriale, vendetta).
- Teppismo.

Soluzione

Il componente Firewall del servizio "Antivirus Dr.Web":

- permette di proibire la scansione della rete e le connessioni al desktop remoto;
- ostacola le intrusioni di hacker attraverso le porte aperte;
- protegge da accesso non autorizzato;
- riduce il rischio di hacking attraverso le vulnerabilità;
- previene il furto di dati attraverso la rete;
- blocca connessioni sospette a livello di pacchetti e di applicazioni;
- il filtraggio a livello di applicazioni consente di controllare l'accesso alla rete da parte di singoli programmi e processi e di registrare tali tentativi di accesso nel log delle applicazioni;
- il filtraggio a livello di pacchetti consente di controllare l'accesso a Internet a prescindere dai programmi che avviano la connessione. Il log del filtro pacchetti conserva le informazioni sui pacchetti trasmessi attraverso le interfacce di rete.

Attenzione!

Di default, Firewall Dr.Web non si installa. Per installare questo componente, è necessario selezionare l'opzione corrispondente durante l'installazione.

Protezione da attacchi mediante vulnerabilità

Minaccia

- Una vulnerabilità è una falla di software che può essere sfruttata per compromettere l'integrità del software o metterlo fuori servizio.
- Tutti i programmi informatici hanno vulnerabilità. Non esiste un programma senza vulnerabilità.
- Per penetrare nel computer remoto, i creatori di virus moderni sfruttano le falle non solo dei sistemi operativi, ma anche delle applicazioni (browser, programmi da ufficio, per esempio, Adobe Acrobat Reader, ed estensioni di flash per i browser).

Da notare!

Oggi l'antivirus è l'unico software moderno che può liberare il sistema operativo da programmi malevoli intrufolatisi attraverso vulnerabilità.

Best practice

Aggiornare periodicamente le applicazioni installate sul computer è altrettanto vitale che aggiornare il sistema operativo. In linea massima, qualsiasi errore nel codice di un programma può essere sfruttato per causare danni al tutto il sistema d'informazione. In questo caso non importa che si tratti di un fallimento transitorio o di seri danneggiamenti dei dati. Per evitare danni, è necessario controllare lo stato dei programmi installati e scaricare tempestivamente gli aggiornamenti e le nuove versioni.

Soluzione

Tramite il monitoraggio HTTP SpIDer Gate e il mail monitor SpIDer MailD è possibile prevenire che oggetti malevoli si infiltrino nel sistema d'informazione attraverso le vulnerabilità dei programmi (quali browser, Adobe Flash, Adobe Acrobat, client di posta) poiché l'intero traffico, compreso quello criptato, viene controllato prima della sua consegna a un programma.

Protezione da infezioni causate tramite tecniche di ingegneria sociale

Il virus informatico più temibile è l'utente.

Saggezza popolare

La maggior parte dei programmi malevoli moderni non possiede una funzione di proliferazione automatica. I creatori di virus fanno affidamento alla distribuzione dei loro "prodotti" da parte degli utenti stessi.

Sono proprio gli utenti che involontariamente aiutano al malware a penetrare nella rete locale dell'azienda. Alcuni utenti non conoscono le nozioni di sicurezza informatica, altri potrebbero essere stanchi e perdono concentrazione — tutto questo potrebbe portare alla violazione delle politiche di sicurezza aziendali. I dipendenti utilizzano periferiche USB, aprono in modo automatico email arrivate da mittenti sconosciuti, navigano sul web senza alcune restrizioni nel tempo lavorativo e così via.

Per indurre gli utenti a distribuire i cavalli di troia, i malintenzionati ricorrono alle tecniche di ingegneria sociale. Esiste una grande varietà di trucchi ideati per ingannare l'utente e farlo avviare il programma malevolo: collegamenti phishing, email false dalle banche o dagli amministratori di qualche risorsa web e altro ancora. Gli svariati metodi di social ingeneering hanno sempre lo stesso scopo, ovvero cercano di ottenere i dati personali sensibili dell'utente, quali password dei servizi web, informazioni riservate o finanziarie.

Best practice

Non ci vuole molto per far fronte ai truffatori che praticano il social engineering. Il rischio di perdere informazioni si riduce se si osservano queste regole semplici:

1. Se avete ricevuto un'email con la richiesta di inviare la Vostra password da qualsiasi risorsa web, cancellate quest'email nonostante le intimidazioni contenuteci (quali la rimozione dell'account, l'azzeramento del conto ecc.). **Gli amministratori delle risorse di rete e le banche non richiedono MAI dati dagli utenti.**
2. Se avete ricevuto da un Vostro amico un'email o un messaggio da contenuti strani che include anche un collegamento a qualche risorsa di rete, metteteVi in contatto con quest'amico in un altro modo (per esempio, telefonandogli) e domandategli perché Vi ha spedito quel messaggio. Probabilmente, il suo account è stato compromesso e viene utilizzato dagli hacker.
3. Se una risorsa web sconosciuta Vi propone di passare a una pagina su cui inserire i Vostri credenziali o dati personali (per esempio, un link che condurrebbe a facebook.com), digitate manualmente il testo del collegamento nella finestra del browser — in questo modo potete essere sicuri che non arriviate a un sito di phishing (si deve tenere presente che vi sono tantissimi metodi per mascherare i veri percorsi dei collegamenti ipertestuali). Prima di digitare il collegamento nel browser, accertateVi che il nome di dominio proposto coincida con il nome di dominio originale (per attirarVi nella trappola, il collegamento malevolo potrebbe contenere, restando al nostro esempio, amicisufacebook.it invece di facebook.com).
4. Se avete letto sul web una notizia che racconta, per esempio, di un nuovo modo per leggere SMS di altre persone, non cercate di attuare questo nuovo metodo. I pirati informatici non svelano mai le falle che hanno trovato. Con tale notizia, sfruttando la curiosità degli utenti, gli hacker vogliono indurrli a vistare una risorsa infettata.
5. Non disattivate il monitoraggio HTTP dell'antivirus (controllo degli indirizzi del web). Questo modulo difende le Vostre attività nella rete.

Importante!

Non disattivate il file monitor SpIDer Guard! Deve stare residente nella memoria del computer e prevenire infezioni controllando file prima dell'avvio e tutti i processi di sistema. SpIDer Guard è un modulo efficace che difende da minacce conosciute e anche da quelle ancora sconosciute utilizzando l'analisi euristica. Ma anche se un nuovo virus non viene rilevato da SpIDer Guard, non potrà eseguire azioni malevole perché verranno impedite dalle tecniche preventive dell'antivirus.

Obiettivo №17

Ridurre periodi di inattività causati da virus

I virus e lo spam sono le principali minacce alla sicurezza informatica per le imprese di qualsiasi tipo e dimensione. Pertanto, il personale del reparto IT ogni giorno deve analizzare lo stato della rete locale dell'azienda, impedire attacchi di virus e superare le conseguenze di incidenti. Tra gli obiettivi fondamentali degli amministratori di sistema è quello di ridurre il tempo durante il quale i dipendenti non possono lavorare perché i loro computer sono stati infettati da programmi malevoli. Da questo compito dipendono il successo dell'azienda e la sua buona reputazione tra i clienti e partner.

Minaccia

- I periodi di inattività sono in media due ore al mese per un dipendente.
- Il più alto è l'impiego di un dipendente, il più costa il suo tempo lavorativo, quindi l'azienda perde di più se non lavora.

Il tempo di inattività è sprecato in attesa. Il dipendente aspetta che il problema venga risolto o persino cerca di risolverlo da solo, il che potrebbe portare a conseguenze imprevedibili, compresa una rovina completa dei dati.

Soluzione

Se l'antivirus si usa come un servizio:

- il software antivirale si aggiorna automaticamente e si gestisce centralmente dal fornitore del servizio o dall'amministratore di sistema dell'azienda;
- i periodi di inattività sono esclusi perché gli utenti non possono eseguire azioni sbagliate in caso di un'infezione presente sul computer – se abilitata l'opzione che impedisce la modifica delle impostazioni dell'antivirus da parte degli utenti.

Il servizio "Antivirus Dr.Web" è un potente strumento per ridurre periodi di inattività lavorativa causata da programmi malevoli.

Dr.Web anti-virus protection system

Servizi

Avvisi di eventi inviati dal sistema di protezione

Il sistema di protezione Dr.Web invia avvisi di problemi verificatisi nella rete antivirale, per esempio, attacchi di virus, avvisi di sistema, messaggi con i risultati di una scansione. Gli avvisi si inviano per email o tramite i mezzi di sistema di Windows a banda larga. I template dei messaggi possono essere personalizzati.

Servizio di invio dei messaggi istantanei

L'interfaccia di invio messaggi consente all'amministratore di sistema di spedire messaggi a singoli utenti o a gruppi di utenti. Si può usare questa funzione per spedire avvisi di epidemia, le istruzioni come comportarsi in caso di un'infezione presente sul computer, messaggi tecnici su problemi nella rete o persino gli auguri di una festa.

Statistiche e report

Il sistema di protezione fornisce agli amministratori le informazioni dettagliate sullo stato della rete antivirale. Qui riportiamo i tipi di informazioni disponibili:

- virus rilevati (un elenco degli oggetti infetti, le minacce, le azioni dell'antivirus ecc.);
- informazioni sui virus rilevati sulle postazioni raggruppati per il tipo di virus;
- informazioni riguardanti i database virali: nome del file che contiene un database virale, versione del database virale, numero di record nel database, data di creazione;
- elenco degli errori di scansione occorsi su una postazione in un periodo;
- elenco dei componenti avviati su una postazione;
- uno stato delle postazioni non regolare che potrebbe esigere l'intervento da parte dell'amministratore, in un periodo;
- elenco dei task assegnati a una postazione in un periodo;
- informazioni dettagliate su tutti i moduli dell'antivirus Dr.Web, quali: descrizione del modulo, nome di funzione, file del modulo, versione completa del modulo ecc.
- elenco delle installazioni del software su una postazione;
- statistiche complessive.

È possibile raccogliere e analizzare su una base regolare le informazioni statistiche di tutte le postazioni della rete antivirale. Le informazioni possono essere presentate in grafici, quindi è possibile creare relazioni illustrate a seguito di un monitoraggio della rete.

Log di verifica azioni

Consente di tenere traccia di tutte le azioni dell'amministratore di sistema quando installa o configura il software antivirale. Se l'amministratore deve spiegare perché ha eseguito determinate azioni, può presentare una relazione completa sul lavoro svolto. Il log di verifica rende trasparenti le azioni che l'amministratore esegue nel sistema di protezione antivirale.

Importante!

Quando si indaga su incidenti informatici, il log di verifica azioni è una prova.

Conclusione

Doctor Web

Doctor Web è un produttore russo che sviluppa sotto il marchio Dr.Web programmi antivirus per la protezione dell'informazione. I nostri programmi sono in continuo progresso dal 1992. Doctor Web è un'azienda all'avanguardia nel suo settore che offre prodotti capaci di soddisfare un'esigenza essenziale dell'impresa odierna – quella della sicurezza dell'informazione.

Siamo uno dei pochi fornitori di antivirus nel mondo che possiedono le proprie tecnologie uniche di rilevamento e trattamento di programmi malevoli. Abbiamo un laboratorio antivirale, un servizio di monitoraggio globale alla ricerca dei virus e un servizio di supporto tecnico.

I nostri programmatori prestano molta attenzione allo sviluppo di tecnologie di protezione contro le minacce sia conosciute che sconosciute. Il sistema di protezione antivirale Dr.Web consente ai sistemi d'informazione dei nostri clienti di resistere validamente a qualsiasi minaccia informatica, persino a una non conosciuta ancora. Le soluzioni Dr.Web soddisfano per l'intero le esigenze delle aziende riguardanti la sicurezza dell'informazione.

Doctor Web ha creato modelli di business innovativi basati sulle sue tecnologie. Nel 2007, siamo stati i primi a introdurre sul mercato russo il nuovo modello di distribuzione dell'antivirus come servizio. Da quel momento è iniziata nell'industria antivirale russa l'epoca di Software come Servizio, e fino ad oggi Doctor Web rimane il leader incondizionato sul segmento relativo di mercato.

Doctor Web dimostra un tasso superiore di crescita annuale delle vendite rispetto agli indici medi del settore. Utenti privati da ogni area del mondo, piccole imprese, aziende maggiori si fidano dei prodotti Dr.Web per molti anni. I certificati e premi dello Stato, nonché la geografia degli utenti di Dr.Web provano l'elevata qualità dei prodotti creati dai dotati programmatori russi.

Informazioni per il contatto

Russia

Doctor Web
Russia, 125124, Mosca, la 3° via Yamskogo polya, 2-12A
Tel: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97
www.drweb.com | www.av-desk.com | www.freedrweb.com | mobi.drweb.com

China

Doctor Web Software Company (Tianjin), Ltd.
112, North software tower, № 80, 4th Avenue, TEDA, Tianjin, China
天津市经济技术开发区第四大街80号软件大厦北楼112
Tel: +86-022-59823480
Fax: +86-022-59823480
E-mail: D.Liu@drweb.com
www.drweb.com

Francia

Doctor Web France
333 b Avenue de Colmar, 67100 STRASBOURG
Tel: +33 (0) 3-90-40-40-20
Fax: +33 (0) 3-90-40-40-21
www.drweb.fr

Germania

Doctor Web Deutschland GmbH
Rodenbacher Chaussee 6, D-63457 Hanau
Tel: +49 (6039) 939-5414
Fax: +49 (6039) 939-5415
www.drweb-av.de

Giappone

Doctor Web Pacific, Inc.
NKF Kawasaki building 2F, 1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken
210-0005, Japan
Tel: +81 (0) 44-201-7711
www.drweb.co.jp

Kazakistan

Doctor Web – Central Asia
Republic of Kazakhstan, 050009, Almaty, Shevchenko, 165b office 910
Tel: +7 (727) 323-62-30, 323-62-31, 323-62-32
www.drweb.kz

Ucraina

Doctor Web Technical Support Centre
Office 3, 4 Kostelnaya str., Kiyev 01001, Ukraine
Tel./fax: +38 (044) 238-24-35, 279-77-70
www.drweb.ua