

Top 10 van tips

waarmee uw kleine onderneming veilig blijft

Het is een ongelooflijk gecompliceerde taak geworden om uw onderneming te beschermen tegen de meest recente internetbedreigingen. Door de gevolgen van aanvallen van buitenaf, interne inbreuken op de beveiliging, en internetmisbruik staat beveiliging hoog op de agenda bij kleine ondernemingen. Wat moet u daarom weten over beveiliging en wat zijn de belangrijkste elementen waarop u zich moet richten? Trend Micro werpt wat licht op dit lastige onderwerp.



1 SLUIT UW DEUREN VOOR MALWARE

U zult het niet in uw hoofd halen om 's nachts uw achterdeur open te laten staan. Dan laat u toch ook geen cybercriminelen toe tot uw onderneming? Dit is echter mogelijk precies wat u doet door uw computers niet te beveiligen met bijvoorbeeld adequate firewalls en antivirussoftware.

NACHA, een Amerikaanse vereniging voor elektronische betalingen, heeft zelfs een waarschuwing doen uitgaan over het toegenomen aantal aanvallen op kleine ondernemingen. *ComputerWorld* meldt: "In het bericht van NACHA werd gesteld dat cybercriminelen zich klaarblijkelijk richten op kleine ondernemingen omdat hier krachtige verificatieprocedures, transactiecontrolemechanismen en rapportage met behulp van 'rode vlaggen' vaak ontbreken. In sommige gevallen, aldus het bericht, verleiden hackers medewerkers van kleine ondernemingen ertoe om phishing-sites te bezoeken. Deze lijken op de website van de financiële instelling van de onderneming, waar ze zich met hun referenties zouden aanmelden."

Malware is schadelijke software die is ontworpen om een pc of netwerk te infiltreren of beschadigen zonder dat u dit weet of hiervoor toestemming hebt verleend.

- **Pas de firewall toe.** Een goede internetrouter heeft een geïntegreerde firewall (dus vergeet niet deze in te schakelen), maar dit is tegenwoordig niet meer voldoende gezien de complexiteit van malware.
- **Bescherm de pc.** De beste beveiligingssoftware gaat verder dan standaard bescherming en is geïnstalleerd op de pc zonder dat de prestaties van de pc, de laptop of het netwerk afnemen. De beste bescherming omvat identiteitsdiefstal, riskante websites en aanvallen van hackers in één oplossing.
- **Weet waartegen u zich moet verdedigen.** Kies een oplossing uit waarmee u mobiele gebruikers en al uw pc's en servers vanaf een enkele console in de gaten kunt houden.
- **Maak het mobiele gebruikers gemakkelijk.** Goede beveiligingssoftware beschikt over plaatsbepalingsmogelijkheden. Hiermee worden de beveiligingsinstellingen op laptops automatisch aangepast aan het optimale beschermingsniveau voor medewerkers, afhankelijk van of deze zich op kantoor of elders bevinden.
- **Schoon e-mail op.** Met antispam wordt de hoeveelheid ongewenste e-mail verminderd, worden risico's geblokkeerd en worden medewerkers minder snel afgeleid. Houd spam tegen voordat deze uw onderneming bereikt.

2 LEG UW BELEID VAST

Denkt u dat uw onderneming te klein is om interessant te zijn voor hackers? Niets is minder waar. De omvang is totaal niet belangrijk voor internetcriminelen en -fraudeurs. Kleinere ondernemingen zijn bovendien een eenvoudiger doelwit omdat IT-resources overbelast zijn. Daarom is het van belang dat uw onderneming beveiliging serieus neemt: blijf medewerkers onafgebroken wijzen op uw veiligheidsvoorschriften. Leg het beleid vast. Geef het door. Dwing het af.

Uw beleid moet onder meer het volgende bevatten:

- **Geef aan wat wel en niet is toegestaan.** Welke toepassingen mogen worden geïnstalleerd op bedrijfscomputers en welke niet?
- **Stel sterke wachtwoorden verplicht.** Verwijs naar tip 4 over wachtwoorden.
- **Leg consequenties op.** Wat gebeurt er als het beleid niet wordt nageleefd? Wees erop voorbereid om uw woorden kracht bij te zetten.
- **Maak er gebruik van. Misbruik het niet.** Wat is gepast gebruik van een door de onderneming ter beschikking gestelde computer? Hiertoe behoort ook het gebruik van internet.
- **Verstrek informatie over e-mail.** Ga in op interne en externe communicatie alsmede welke berichten wel en niet mogen worden geopend of doorgestuurd.
- **Versleutel of wees helder.** Besluit of en wanneer een oplossing voor het versleutelen van e-mail vereist is om gevoelige gegevens te beschermen.
- **Wijs een aanspreekpunt aan.** Bij wie kunnen medewerkers terecht als ze vragen hebben over het beleid of over computerbeveiliging in het algemeen?

3 PAK SOCIALE MEDIA AAN VOORDAT U EROVER STRUIKELT

Sociale media zijn niet meer weg te denken, dus bied uw medewerkers 'best practices' en richtlijnen. Op de volgende manieren kunt u risico's in sociale netwerken tot een minimum beperken:

- **Kijk wie het zegt.** Bepaal wie namens het bedrijf mogen spreken en geef alleen deze medewerkers toestemming om over de interne en externe gebeurtenissen te schrijven.
- **Bepaal wat vertrouwelijk is.** Zorg ervoor dat sociale media als Facebook, Twitter en LinkedIn zijn opgenomen in uw geheimhoudingsverklaring voor vertrouwelijke bedrijfsgegevens.

- **Bied richtlijnen en een forum om deze te ontwikkelen.** Bij blogs en publicaties voor het bedrijf door middel van sociale media moet in richtlijnen zijn vastgelegd welke informatie is toegestaan en wie artikelen mag publiceren. Richtlijnen moeten verder gaan dan alleen beveiliging:
 - Bloggers moeten zich identificeren als iemand die werkt bij of wordt betaald door uw bedrijf. Anders keert dit zich tegen u.
 - Stel de toon van het blog vast.
 - Bescherm gegevens en de gevoelens van klanten. Herinner klanten eraan dat persoonlijke gegevens niet in een publicatie mogen worden gedeeld en geef aan waar ze terecht kunnen met vragen over vertrouwelijke gegevens.
 - Bepaal wanneer informatie over ondersteuning moet worden vrijgegeven in sociale media.
 - Zorg voor steun van directie/eigenaren zodat richtlijnen snel kunnen worden aangepast zonder de zakelijke behoeften uit het oog te verliezen.
 - Gebruik resources als BlogWell (www.blogwell.com) om richtlijnen op te stellen en meer informatie over sociale media te verkrijgen.
- **Wees sociaal, maar denk na.**
 - Publiceer alleen informatie als u volstrekt geen probleem ermee hebt dat deze een brede verspreiding krijgt, afhankelijk van wat u wilt bereiken.
 - Ga uit van het ergste om de beste resultaten te verkrijgen. Stimuleer medewerkers om online zo min mogelijk persoonlijke gegevens te delen voor hun eigen veiligheid en die van uw bedrijf.
 - Voeg alleen vertrouwde personen toe aan de lijst met contactpersonen.
 - Klik niet op onverwachte koppelingen die afkomstig zijn van onbekenden.
 - Vertrouw nooit iemand volledig die u niet zo goed kent.

4 BEVEILIG MET WACHTWOORDEN

Of u het nu leuk vindt of niet: wachtwoorden zijn de sleutel tot de meeste netwerken van kleine ondernemingen, dus ze zijn belangrijk bij de bescherming van de toegang tot uw netwerken. U hoeft geen statisticus te zijn om te weten dat een wachtwoord sterker is naarmate u er meer tekens voor gebruikt.

- **Sta op sterkte.** Stel sterke wachtwoorden van minstens acht tekens met cijfers erin verplicht, zodat u eenvoudige aanvallen kunt tegenhouden waarbij wachtwoorden worden geraden.
- **Tijd voor verandering.** Stel een verloopdatum voor oude wachtwoorden in en leg op dat wachtwoorden regelmatig moeten worden gewijzigd.
- **Stel ze veilig.** Leg medewerkers uit waarom het bedrijf gevaar loopt als ze wachtwoorden noteren, wachtwoorden opslaan op een mobiele telefoon of een wachtwoord gebruiken dat gemakkelijk kan worden geraden.
- **Vind de combinatie.** Voor de sterkste wachtwoorden gebruikt u helemaal geen woorden. Gebruik willekeurige letters, cijfers en speciale tekens. Maak zo nodig een patroon op uw toetsenbord. qWe4%6yUi is veel sterker dan golrish#3.

5 WEES KRITISCH OVER INTERNETBEVEILIGING

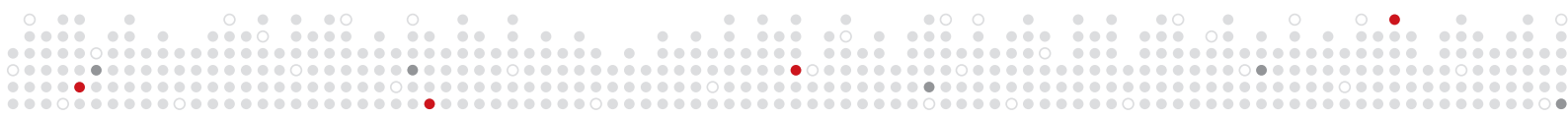
Internet biedt ondernemingen fantastische mogelijkheden. Maar internet kan u ook meer openstellen voor malware als uw beveiligingssoftware niet content op een proactieve manier scant om malware op te sporen en u attendeert op mogelijke problemen. Selecteer beveiligingsoplossingen waarmee u de nieuwste bedreigingen kunt bestrijden zonder uw medewerkers af te leiden:

- **Stop de onzinnige koppelingen.** Ga er niet van uit dat medewerkers nadenken over beveiliging en hun toegang tot het netwerk of internet beperken. Automatiseer updates en maak beveiliging transparant voor medewerkers.
- **Houd het web productief.** Stel niet alleen richtlijnen voor aanvaardbaar internetgebruik op, maar selecteer ook oplossingen waarmee onaanvaardbaar gebruik wordt tegengegaan. Met URL-filtering kunt u de toegang tot onproductieve sites volledig of in werktijd beperken en verdedigen tegen riskante koppelingen, zodat uw onderneming, medewerkers en gegevens in eigen handen blijven en niet in handen van identiteits- of gegevensdieven vallen.

6 VRAAG MEDEWERKERS OM HULP

Iedereen kent wel de koppen over gevallen waarbij belangrijke gegevens verloren zijn gegaan. Wist u echter dat wel 80% van alle gegevensverlies wordt veroorzaakt door een menselijke fout (doordat vertrouwelijke of gevoelige gegevens naar de verkeerde persoon of onbeveiligd worden verzonden)?

- **Naleven om te overleven.** Overleven is misschien wat overdreven, maar de gevolgen van gegevensverlies en het onopzettelijk weglekken van informatie worden steeds groter naarmate de regelgeving strenger wordt. Informeer medewerkers dus over de vereisten van de regelgeving en 'best practices' voor de bescherming van gegevens. Leg uit wat de risico's zijn als de regels niet worden nageleefd. Laat hen weten dat het hun taak is om de risico's te beperken door waakzaam te blijven.
- **Leg medewerkers uit waarom ze belangrijk zijn.** Als medewerkers scans niet uitvoeren of ongepast materiaal verzenden, kan de onderneming te maken krijgen met malware, rechtszaken en beschadiging van de reputatie.
- **Houd informatie vertrouwelijk.** Laat alle medewerkers weten welk type informatie vertrouwelijk is en welke problemen zich kunnen voordoen als dergelijke documenten of bestanden in de openbaarheid komen.



7 LAAT UW RESELLER/CONSULTANT VOOR U WERKEN

Als u een goede relatie met uw IT-reseller/-consultant hebt, beschikt u altijd over een betrouwbare adviseur die u om hulp kunt vragen bij IT-problemen.

- **Vraag om meer.** De reseller of consultant met wie u samenwerkt moet niet alleen de beste prijs bieden of promoties bij u aanprijzen, maar ook objectieve adviezen over uw IT-infrastructuur kunnen verstrekken. Ze kunnen en moeten u helpen bij het kiezen van de juiste oplossing voor uw onderneming. Een oplossing die meegroeit met uw behoeften en uw IT-investering beschermt. Anders wordt het misschien tijd voor een ander.
- **Besteed beheer uit.** Uw reseller of consultant biedt mogelijk zelfs aan om uw beveiligingsoplossing op afstand voor u te beheren. Dit betekent minder rompslomp en zelfs een betere bescherming voor u en uw onderneming. Laat weten dat beveiliging een belangrijke taak is voor iedere medewerker.

8 GEEF HET VOORBEELD

Als u uw woorden niet nakomt, zullen anderen dat ook niet doen. Of u nu wel of niet een positie van leiderschap bekleedt, mensen kijken wat iedereen om hen heen doet. Eén persoon kan al verschil maken.

- **Wees niet de schuldige.** Er is maar één persoon nodig om een vervelend virus door het hele bedrijf te verspreiden.
- **Laat van u horen.** Als u een betere beveiligingsmethode hebt ontdekt of iets hebt gehoord over een nieuwe opkomende bedreiging, laat anderen dit dan weten. Deel 'best practices' met afdelingen.

9 BLIJF UP-TO-DATE

Zorg ervoor dat uw mobiele gebruikers, pc's en servers gebruikmaken van de best mogelijke informatie over bedreigingen. Met handmatige of onregelmatige updates van uw beveiligingssoftware zet u de deur open voor bedreigingen. Het cliché is waar: u bent net zo veilig als uw laatste update.

- **Ontlast uw pc's.** Als uw beveiligingsoplossing uw pc's vertraagt, geldt dat niet alleen voor u. Dit is een vaak gehoorde klacht over conventionele beveiligingsoplossingen. Zoek oplossingen waarbij het datacenter van de leverancier het werk voor u doet door middel van gehoste technologieën. Laat uw pc's en servers uw zakelijke activiteiten afhandelen, niet uw beveiliging.
- **Vertrouw niet op een oud antivirusprogramma.** In traditionele antivirusprogramma's werden bedreigingen gedetecteerd door bestanden te vergelijken met vingerafdrukken of 'handtekeningbestanden' op elke computer. Nieuwe bedreigingen nemen echter exponentieel toe (meer dan 2000% sinds 2004). Door meer handtekeningbestanden te verzenden, slibben uw pc's gewoon dicht. Met nieuwe detectiemethoden wordt het equivalent van achtergrondcontroles uitgevoerd op afzenders van e-mail, bestanden en websites. Zodoende wordt een betere en snellere beveiliging geboden zonder uw pc's te vertragen.
- **Zorg dat het besturingssysteem automatisch wordt bijgewerkt.** Maak het zo eenvoudig mogelijk om ervoor te zorgen dat uw pc's over de nieuwste patches beschikken. De kwetsbare plekken in uw besturingssysteem zijn een belangrijke factor bij aanvallen. Zorgt er daarom voor deze patches snel en automatisch worden ingezet.
- **Controleer of verplichte patches zijn geïnstalleerd.** Verstrek uw gebruikers details over benodigde softwareversies en de wijze waarop ze kunnen bepalen wat hun huidige versie is. Verstrek koppelingen en aanwijzingen voor het bijwerken naar de juiste versie. Als gebruikers zien dat u naleving van het beleid serieus neemt, zullen ze het eerder zelf naleven.

10 KIES EEN BEVEILIGINGSPARTNER, NIET ALLEEN EEN LEVERANCIER

Selecteer een leverancier die inzicht heeft in de unieke aspecten van de beveiliging van een kleine onderneming.

- Kies een beveiligingsleverancier. Ga na of uw leverancier beveiliging als kernactiviteit heeft, of het eraan doet.
- Controleer de staat van dienst. Leveranciers met een jarenlange staat van dienst, waarbij ze bescherming tegen meerdere bedreigingen bieden en kennis van zowel kleine als grote ondernemingen hebben, kunnen het beste uw beveiliging ondersteunen.

RESOURCES

- TrendWatch biedt educatieve video's, technische verslagen en meer: <http://us.trendmicro.com/us/trendwatch/>
- www.worryfree.com biedt video's en informatie over producten van Trend Micro die speciaal zijn ontworpen voor kleine ondernemingen.

NEEM DE VOLGENDE STAPPEN

Gebruik de onderstaande checklist om te bepalen op welke punten uw bedrijf goed presteert. Bepaal vervolgens welke stappen u nu wilt nemen.

TIP

1. Sluit uw deuren voor malware

VINK AFGERONDE STAPPEN AF

- ☐ Installeer en gebruik een beveiligingsoplossing die u beschermt tegen meerdere bedreigingen (zoals virussen, webbedreigingen, spyware en bots)
- ☐ Selecteer een oplossing waarmee pc's en servers, op de eigen locatie en elders, kunnen worden bekeken en beheerd
- ☐ Weet wat wordt beschermd door een oplossing te kiezen met een enkele console voor gebruikers elders, interne pc's, en bestands- en mailservers
- ☐ Maak het mobiele gebruikers gemakkelijk door oplossingen met plaatsbepaling te selecteren
- ☐ Schoon e-mail op met antispam

2. Leg uw beleid vast

- ☐ Leg uw beleid schriftelijk vast. (Zo belangrijk is het!)
- ☐ School medewerkers en behandel het beleid voor IT-beveiliging als contract
- ☐ Leg de consequenties op als het beleid niet wordt nageleefd
- ☐ Bepaal wat medewerkers wel en niet mogen doen met bedrijfs-pc's
- ☐ Informeer over 'best practices' voor e-mail om phishing en spam te voorkomen
- ☐ Versleutel e-mail zo nodig om de inhoud te beschermen
- ☐ Wijs een aanspreekpunt of primaire contactpersoon voor IT-beveiliging aan

3. Pak sociale media aan

- ☐ Bepaal wie blogartikelen over het bedrijf mogen publiceren
- ☐ Geef aan wat vertrouwelijke en openbare informatie is
- ☐ Bied richtlijnen en een forum om deze te ontwikkelen
- ☐ Wees sociaal, maar denk na over welke informatie uw medewerkers openbaar maken

4. Begin met wachtwoorden

- ☐ Stel sterke wachtwoorden verplicht
- ☐ Stel een verloopdatum voor wachtwoorden van gebruikers
- ☐ Bewaar wachtwoorden op een veilige plaats, niet op een Post-It of iPhone
- ☐ Combineer letters en cijfers om dieven tegen te houden

5. Wees kritisch over internetbeveiliging

- ☐ Plaats is belangrijk, dus zorg ervoor dat medewerkers elders eenvoudig kunnen worden beschermd door middel van oplossingen met plaatsbepaling
- ☐ Stel de bescherming zo in dat riskante en onproductieve websites automatisch worden geblokkeerd

6. Vraag medewerkers om hulp

- ☐ Leef voorschriften en aanbevolen beveiligingsprocedures na
- ☐ Leg uit waarom medewerkers belangrijk zijn voor de beveiliging
- ☐ Implementeer beveiligingsrichtlijnen
- ☐ Benadruk nogmaals wat vertrouwelijk is

7. Laat resellers/consultants voor u werken

- ☐ Vraag om meer dan het uitvoeren van een bestelling; zoek een zakenpartner die een betrouwbare adviseur kan zijn
- ☐ Besteed beveiligingsbeheer uit aan uw reseller/consultant, zodat u waardevolle tijd en energie weer in uw onderneming kunt steken

8. Geef het voorbeeld

- ☐ Eén persoon kan het verschil maken, dus meet uw acties af aan het beleid
- ☐ Zoek een betrouwbaar informatiepunt voor beveiliging en raadpleeg dit eenmaal per week

9. Blijf up-to-date

- ☐ Ontlast uw pc door een oplossing te kiezen die gehoste verwerking in een datacenter biedt
- ☐ Vertrouw niet op een oud antivirusprogramma; gebruik meerdere detectieprocessen
- ☐ Zorg dat het besturingssysteem automatisch wordt bijgewerkt
- ☐ Controleer of verplichte patches zijn geïnstalleerd

10. Kies een beveiligingspartner

- ☐ Selecteer een leverancier die op beveiliging is gericht
- ☐ Controleer de staat van dienst van een leverancier en kies een gerenommeerd bedrijf dat ervaring heeft met grote en kleine ondernemingen

Voor meer informatie kunt u contact opnemen met uw Trend Micro Account Manager of gaan naar: www.worryfree.com.