Whitepaper

KASPERSKY lab

TIEN MANIEREN
waarop de IT-afdeling cybercrime toelaat

Be Ready for What's Next.

Tien manieren waarop de IT-afdeling cybercrime toelaat

We hopen dat u het artikel ‚De slag om ~~het eindpunt~~' van Kaspersky Lab inmiddels hebt gelezen. Zo niet, download dit artikel dan voordat u verder gaat (in de bronnensectie). ‚De slag om ~~het eindpunt~~' gaat over het werkelijke doelwit van cybercriminelen anno nu: ~~het eindpunt~~ of de medewerker. In dit artikel wordt besproken hoe IT-personeel nietsvermoedend cybercrime toelaat door cybercriminelen toegang te geven tot systemen en gegevens door een reeks aan misvattingen en valse aannames.

Eisen van eindgebruikers voor toegang tot internet en alle communicatiemethoden die daarmee mogelijk zijn, zijn hoger dan ooit. De zakelijke vraag naar deze communicatiemethoden is ook in opkomst. De mobiliteit van medewerkers en bedrijfsgegevens zorgen voor een groeiende uitdaging en het is moeilijk om de exponentieel groeiende bedreiging van cybercrime voor te blijven. Als gevolg daarvan zijn veel IT-afdelingen medeplichtig geworden aan cybercrime, vaak zonder dat ze dat weten of er veel van begrijpen. In dit document wordt uitleg gegeven over verschillende manieren waarop IT-afdelingen cybercrime toelaten in onze omgevingen. Het geeft richtlijnen om te voorkomen dat deze gevaarlijke en vernietigende praktijk doorgaat.

Er worden 10 manieren besproken waarop IT-afdelingen cybercrime toelaten. Ook worden er manieren besproken om cybercriminelen te stoppen, gebaseerd op onderzoek door derden en analyse door experts bij Kaspersky Lab. Hoe is uw organisatie opgewassen tegen deze maar al te algemene valkuilen?

Manier #1
Aannemen dat gegevens zich in het datacentrum bevinden

Sta er eens bij stil dat de meeste leidinggevenden hun e-mails op hun smartphone (iPhone, BlackBerry, enz.), hun laptop én op de mailserver van hun bedrijf bewaren. Dan wilt u al snel met ons aannemen dat er twee keer zoveel gegevens buiten het datacentrum zijn als binnen het datacentrum. Tel daar alle USB-sticks, cd's, back-upschijven, cloud-based oplossingen en gegevensuitwisseling met zakelijke partners bij op en dit cijfer groeit verder dan we normaliter beseffen.

We realiseren ons dat deze gegevens niet van de buitenwereld afgesloten zijn, maar IT-afdelingen behandelen ze alsof dat wel zo is. Waarom zouden we anders zoveel tijd en geld investeren in het versterken van de omtrek van het datacentrum, met technologieën zoals verificatie, toegangsbeheer, firewalls, netwerkinbraakpreventie, enz.? We willen niet zeggen dat deze technologieën niet belangrijk zijn. Dat zijn ze absoluut. Maar we moeten ons concentreren op waar onze gegevens momenteel staan: op ~~het eindpunt~~.

Gegevens staan niet op vaste plaatsen. Ze verplaatsen zich vrij buiten de datacentra. IDC-onderzoek toont aan dat desktopcomputers/laptops de grootste zorg zijn voor Data Loss Prevention (DLP). ~~Het eindpunt~~ is een directere bedreiging voor gegevensverlies. IDC-gegevens laten ook zien dat mobiliteit de nummer één factor is waarvoor nieuwe beveiligingsuitgaven worden gemaakt. Dit suggereert dat meer organisaties op hun hoede zijn en veiligheidsmaatregelen tot buiten hun datacentrum uitbreiden.

Manier #2
Falen om de waarde van gegevens op mobiele apparaten te herkennen

Uw tijd is kostbaar. De uren die we besteden aan het maken van rapporten en analyseren van gegevens om goede zakelijke beslissingen te nemen, de weekenden waarin we werken aan e-mail en presentaties en het toepassen van due diligence bij zakelijke kansen die tijdgevoelig zijn, zorgen er allemaal voor dat er enorme hoeveelheden gegevens op portable systemen komen te staan. Toch gaan IT-afdelingen met een laptop om alsof het een fles cola betreft. Als een apparaat verloren of gestolen is, wordt alleen de waarde van de lege fles geclaimd. De waardevolle gegevens die op het apparaat stonden, worden vergeten. Daarom gaan productieschema's van mobiele apparaten meestal over de waarde van het apparaat in plaats van de waarde van de gegevens. Het is een feit dat de waarde van de gegevens op het apparaat de waarde van de apparaten vaak overschrijdt. Gegevens zijn vaak kunnen honderden malen meer waard.

Beheerde antimalware, diefstalbeveiliging en privacytechnologie voor mobiele apparaten vormen een goed begin voor het beschermen van mobiele gegevens. De trend onder bedrijven is om gebruikers (vanaf het niveau van leidinggevenden) bij aankoop van een mobiel apparaat zoals laptop of smartphone voor zakelijke doeleinden zelf het merk en model te laten kiezen. Het groeiende aantal iPhones dat wordt ondersteund door zakelijke netwerken is hiervan een goed voorbeeld. Helaas maken veel zakemensen en IT-winkels zich meer zorgen over de kosten en levertijd van vervanging voor het apparaat dan over de waarde van de gegevens op het apparaat.

Medewerkers maken gebruik van een apparaat naar eigen keuze in plaats van een apparaat dat optimaal geschikt is voor beheerde antimalware, diefstalbeveiliging en privacytechnologie. Dat heeft tot gevolg dat er een groeiende verscheidenheid aan apparaten, besturingssystemen, dragers, beveiligingsprofielen en andere technologieën binnen het bedrijfsnetwerk ontstaat. Voor organisaties met een beperkte hoeveelheid beveiligingspersoneel kan de vraag naar beveiliging voor meerdere platformen de capaciteit voor ondersteuning overschrijden.

Manier #3
Laptops en mobiele apparaten behandelen als bedrijfskapitaal, dat nooit persoonlijk wordt gebruikt, zodat bedrijfsgegevens nooit op thuissystemen komen te staan.

We kunnen er niet meer van uitgaan dat bedrijfskapitaal alleen wordt gebruikt voor zakelijk gebruik. De laptop dient voor veel reizende zakenmensen bijvoorbeeld als primair middel voor communicatie en transacties. Dit betekent social networking om relaties te onderhouden, naast toepassingen zoals Skype om betaalbaar internationaal te bellen. Deze ontwikkeling binnen zakelijke IT groeit al jaren. Zoals we al hebben besproken, verwachten medewerkers flexibiliteit en keuzes voor door het bedrijf beheerde apparaten.

Veel medewerkers gebruiken hun persoonlijke computers om buiten werktijd toegang te krijgen tot gegevens. Als deze apparaten niet goed beveiligd zijn, loopt u het risico op breuken in de beveiliging. Gebruiksbeleid en beheerde beveiligingssoftware zijn noodzakelijk om gegevens zoveel mogelijk te beschermen. Persoonlijke apparatuur kan hier ook onder vallen. Veel bedrijven breiden investeringen en licenties voor beveiligingssoftware uit naar hun medewerkers om zo de paraplu van beveiliging groter te maken. Informatie die op mobiele apparaten zoals smartphones, netbooks of laptops is opgeslagen binnen de bedrijfsomtrek moet absoluut gecodeerd worden, omdat deze apparaten gemakkelijk verloren, vergeten of gestolen kunnen worden.

Manier #4
Mobiele apparaten gebruiken als desktopcomputers

Een paar jaar terug werd er een solide omtrek gedefinieerd voor onze IT-netwerken. Beschermingstechnologieën gaven duidelijk aan wat zich binnen in het netwerk bevond en wat extern was, zoals een middeleeuws kasteel met een gracht eromheen. Externe apparaten werden beschouwd als onbetrouwbaar, en interne apparaten profiteerden van de bescherming van de firewall van het bedrijf die als het ware de muren van het kasteel vormde. Wereldwijd zien bedrijven toenemende voordelen in om medewerkers extern of mobiel te laten werken. Vooruitgang in mobiele technologie heeft het voor bedrijven mogelijk gemaakt om een ‚altijd verbonden' medewerker te ontwikkelen, die waarheen de reis ook gaat altijd volledige toegang heeft tot bedrijfsbronnen zoals applicaties, documenten en e-mail. Die toegang geldt ook voor mobiele apparaten. Mobiele medewerkers hebben toegang tot bedrijfsnetwerken en gegevens vanuit lounges op vliegvelden, hotelkamers en internetverbindingen tijdens vluchten... Deze zijn allemaal onbeveiligd. Daarom beperkt de huidige werkdag zich nauwelijks meer van 9 tot 5. Mensen werken, krijgen toegang tot de nieuwste informatie, reageren meteen op contact met klanten en voeren veel meer dagelijkse taken uit. Dit gebeurt de hele dag door. Deze omgeving heeft echter een nieuwe bedrijfskwetsbaarheid veroorzaakt die waarschijnlijk doelwit wordt voor opkomende bedreigingen (Mobile Security – IDC).

Een sterk beveiligingsbeleid voor een laptop verschilt fundamenteel van dat van een desktopcomputer. Vaak hebben desktopcomputers die alleen op de werkplek worden gebruikt bepaalde technologieën zoals individuele firewalls niet nodig. Laptops hebben echter een waarschuwingssysteem nodig dat zich aan situaties aanpast. Als ze de relatieve veiligheid van het bedrijfsnetwerk verlaten, moeten extra beveiligingsfuncties zo geprogrammeerd zijn dat ze automatisch worden ingeschakeld. Beveiligingsmaatregelen zoals een firewall instellen, gebruik van Bluetooth en draadloze verbindingen zonder wachtwoord uitschakelen en verbeterde controle op USB-apparaten moeten automatisch worden ingeschakeld als een laptop buiten het bedrijfsnetwerk wordt gebruikt.

Manier #5
Onbeschermd social media gebruiken

Sociale netwerken zijn blijvend. Deze technologie is de nieuwe ‚must-have'. Delen van uw bedrijf kunnen niet zonder, als ze willen groeien. Ze kunnen dan ook enorm veel opleveren - mits juist toegepast.

Tien jaar geleden stond er druk op IT-afdelingen voor eenvoudige internettoegang. Toen kwam er vraag naar zakelijke e-mail en daarna instant messaging-applicaties. Uiteindelijk werden deze allemaal essentiële bedrijfsmiddelen. Social media is de nieuwe golf, en we moeten erop voorbereid zijn. Veel organisaties worstelen met de vraag hoe ze hun medewerkers verantwoordelijk Web 2.0 kunnen laten gebruiken zonder naleving van beveiligingsbeleid en reglementen op te offeren. Social media en Web 2.0-technologieën kunnen organisaties helpen om samenwerking en productiviteit uit te breiden en de inkomsten te laten groeien. De nadruk moet liggen op hoe organisaties op een veilige manier omgaan met social media, omdat het op een paar uitzonderingen na uiteindelijk onpraktisch is om sociale media volledig uit te bannen.

Een formeel beleid om de toegang en het beheer van social media te beheren is essentieel. Als een bedrijf bijvoorbeeld de omtrek tegen malware-aanvallen beschermt maar niet de toegang tot sociale netwerken niet genoeg beheert, kan de nalatigheid van één medewerker ervoor zorgen dat het bedrijfsnetwerk besmet raakt. Dit kan direct of indirect aanzienlijke economische schade tot gevolg hebben. Sociale netwerken kunnen ook tot een informatielek leiden als medewerkers vrijwillig informatie delen met derden.

Afgezien van enkele zeer gecontroleerde academische omgevingen is het uiteindelijk niet praktisch om sociale media uit te bannen. Het is praktischer om technologie te implementeren die het verkeer op social media-websites nauwkeurig in de gaten houdt en die kwaadaardige websites blokkeert.

Manier #6
Focus op bescherming in plaats van op detectie en reactie

Voor complete beveiligingsplannen zijn meerdere capaciteiten nodig. Deze basismogelijkheden zijn bescherming, detectie en reactie. Antivirusproducten worden vaak over het hoofd gezien, beschouwd als bulkproducten en jaarlijks automatisch verlengd. Het gevolg hiervan is dat de kwaliteit van defectie en de reactiemogelijkheden ook over het hoofd gezien worden. Zoals we hebben laten zien, zijn dit noodzakelijke elementen in uw beveiligingsstrategie. En er is een enorm spectrum van bescherming, functioneren, beheersbaarheid, implementatiemogelijkheid en ondersteuning in de sector.

Veel bedrijven verschuiven de aandacht naar nieuwe beveiligingstechnologieën zoals DLP, codering enz. Dit zijn praktische tools, maar het totale aantal malware-incidenten en besmettingen blijft groeien. Een onderzoek van IDC wees uit dat bij 46% van de organisaties het aantal malware-incidenten is toegenomen, terwijl dit aantal bij slechts 16% van de organisaties daalde. De MKB-omgeving (500–2499 medewerkers) heeft het grootste verschil ervaren. Binnen deze categorie nam malware bij 44% toe en bij slechts 7% nam het af. Dat betekent dat malware nog steeds door de verbeterde preventiemaatregelen glipt en laat zien dat er nog meer nadruk gelegd moet worden op capaciteit voor detectie en reactie. IT-afdelingen hebben geïnvesteerd in beschermingsmechanismen aan de gateway, maar laten de deuren wijd open staan door medewerkers op internet te laten surfen zonder de juiste detectiemechanismen die moeten garanderen dat criminelen worden gedetecteerd en geblokkeerd.

Omdat cybercriminelen het tegenwoordig op ~~het eindpunt~~ hebben voorzien, moet robuuste detectie- en reactietechnologie op ~~het eindpunt~~ worden geïmplenteerd om het te beschermen tegen malware dat door cybercriminelen is ontworpen om (inlog)gegevens en inkomsten te stelen.

Manier #7
Falen om een cultuur van alertheid te onderhouden

Bewustzijn en training van eindgebruikers zijn essentieel in alle stadia en op alle niveaus van informatiebeveiliging. Medewerkers moeten bijvoorbeeld leren hoe ze zich kunnen verdedigen tegen kwaadaardige code: veilig surfen, spyware en scareware vermijden en leren wat de regels voor bijlagen zijn. Wachtwoordbeleid moet worden ingevoerd én worden gehandhaafd. Beleid voor internetgebruik moet duidelijk gecommuniceerd, gecontroleerd en nageleefd worden.

Bewustzijn van bedreigingen, impact en uitbreidingsmethoden van malware zorgt dat gebruikers alert zijn en weerhoudt ze van slechte beslissingen die hun ~~eindpunt~~ kunnen besmetten. Regelmatig terugkerende campagnes voor beveiligingsbewustzijn zijn essentieel. Zo blijven medewerkers geïnformeerd en beschermd. Natuurlijk is het van groot belang dat het IT-personeel goed op de hoogte is van huidige bedreigingstechnologie en aanvalsmogelijkheden, zodat ze verstandige beslissingen kunnen nemen over beschermings- en preventietechnologie.

Manier #8
Te weinig meldingen van gaten in de beveiliging

Hoewel beveiligingsbreuken door cybercrime met meer dan 23% zijn toegenomen en de kosten door deze breuken meer dan verdubbeld is, gaat het hier slechts om het topje van de ijsberg. Deze door de FBI gepubliceerde gegevens zijn misleidend omdat bedrijven vaak geen melding maken van inbreuken. Ze willen simpelweg niet dat iedereen te weten komt dat ze een gat in de beveliging hadden, omdat ze bang zijn dat dit negatieve gevolgen heeft voor hun aandelen, hun waarde, hun merk en hun reputatie.

Deze impuls om het te onderdrukken is natuurlijk, maar het resultaat is een vervormd beeld van de groei van de bedreiging op internet. Door te weinig te rapporteren wekken bedrijven de valse schijn dat de dreiging van malware minimaal is en dat de toename in cybercrime wordt opgeblazen. De realiteit is dat de bedreiging met veel meer 23% is toegenomen. De FBI kan alleen geen betere cijfers geven omdat er te weinig melding wordt gemaakt.

Bedrijven hebben er veel baat bij om te weten welke inbreuken voorkomen hadden kunnen worden, hoe deze tot stand komen en hoe de bedrijven zich tegen een soortgelijke aanval kunnen beschermen.

Manier #9
Genoegen nemen met naleving

Naleving van regels en IT-beveiliging zijn niet altijd synoniem aan elkaar. Ook als u de reglementen goed naleeft kunt u zeer slecht beveiligd zijn. Veel organisaties zien malwarebescherming als iets dat ze kunnen afvinken: “Ik moet het hebben en ik moet het onderhouden, maar dat is alles.”

Naleving van regels vraagt om een top-down aanpak. Een kant-en-klaar sjabloon definieert doorgaans het initiatief. Het bedrijf moet kijken naar producten en procedures om erachter te komen hoe ze het sjabloon kunnen toepassen. Beveiliging is als het op de juiste manier wordt toegepast echter een bottom-up initiatief. Als u een softwareproduct of de architectuur voor het nieuwe netwerk van uw organisatie ontwerpt, moeten hier beveiligingselementen in worden opgenomen. Als u bijvoorbeeld een productarchitectuur ontwerpt, beschrijft u in een eerste versie de communicatie, lokalisatie, versies enz. Zo moet dat ook voor beveiligingselementen gebeuren: ze moeten vanaf dag één worden ingebouwd in de applicatie. De beveiligingselementen moeten door ontwikkeling worden herzien en verbeterd. Naleving van regels kan een vals idee van veiligheid zijn voor wie niet begrijpt hoe moeilijk het is om de digitale zakenwereld te beveiligen. Alleen naleving moet niet het einddoel zijn.

Manier #10
Aannemen dat alles in orde is

Zelfs als systemen veilig zijn, worden ze uiteindelijk door mensen bediend. In veel gevallen ontstaan problemen vanuit het menselijke element: een klein onbedoeld foutje of een gebrek aan kennis en ervaring. Bedrijfspersoneel moet worden getraind in informatiebeheer en bijvoorbeeld leren hoe ze moeten handelen in specifieke situaties, hoe ze een duidelijk en bedrijfsbreed veiligheidsbeleid en de bijpassende procedures moeten volgen, hoe ze malware voorkomen door nauwkeurig en zorgvuldig te zijn en hoe ze, mocht malware al in het netwerk zijn gekomen, juist handelen om gegevens te beveiligen en verder verlies te voorkomen.

Kijk heel goed naar de mogelijkheid van een beveiligingsevenement binnen uw bedrijf. Vrijwel niets is in orde. We moeten beter leren zorgen dat gegevens die essentieel zijn voor het bedrijf niet in verkeerde handen vallen.

Samenvatting

Dagelijks vinden cybercriminelen nieuwe manieren om zakelijke ~~eindpunten~~ te infiltreren, met als enige doel gegevens en geld te stelen. Volgens een rapport van SANS.org met de naam “The Top Cyber Security Risks” verliezen bedrijven duizenden dollars per dag, terwijl ze denken dat ze veilig zijn.

We kunnen allemaal leren hoe we ons bedrijf beter beschermen: zorg dat essentiële gegevens niet in verkeerde handen vallen

Kaspersky Lab B.V.
Papendorpseweg 79
3528 BJ Utrecht
Nederland
sales@kaspersky.nl
www.kaspersky.com
www.threatpost.com

n6ja