



Trend Micro™

Smart Protection Network

Stop webbedreigingen voordat ze u bereiken.
Beveiliging is nu nog slimmer.

Het Trend Micro Smart Protection Network is een "in-the-cloud" infrastructuur van de volgende generatie voor de beveiliging van content op clients die is ontworpen om klanten te beschermen tegen webbedreigingen. Doordat internet- en "in-the-cloud"-technologieën worden gecombineerd met kleinere, lichtere clients, hebt u direct toegang tot de allernieuwste beveiligingshulpmiddelen waar en hoe u ook verbinding maakt, ongeacht of dat thuis, binnen uw ondernemingsnetwerk of onderweg is. Beveiliging die nog weer slimmer is.

PROBLEEM

Internet is uitgegroeid tot een uiterst krachtig platform dat de manier waarop we zaken doen en communiceren heeft veranderd. Het biedt anonimiteit, een toenemend aantal gebruikers en zich ontwikkelende technologieën die nieuwe zwakheden blootleggen die vatbaar zijn voor misbruik. Telkens als we surfen op het web of klikken op een URL die is opgenomen in een e-mailbericht, stellen we onszelf en anderen bloot aan het risico van webbedreigingen. Het huidige samenstel van bedreigingen wordt gekenmerkt door op winst beluste cybercriminelen, die de ontwikkeling van internet hebben aangegrepen voor het opzetten van een krachtige ondergrondse economie. De bedreigingen van vandaag zijn verfijnd en gevaarlijk. Webbedreigingen zijn multidimensionale, gecoördineerde aanvallen die aanzienlijke schade kunnen veroorzaken, met inbegrip van financiële verliezen, identiteitsdiefstal en verlies van intellectueel eigendom of handelsgeheimen om er maar een paar te noemen. Niet alleen uw informatie, maar ook uw persoonlijke en zakelijke reputatie staan op het spel.

Het aantal schadelijke aanvallen is exponentieel toegenomen. In heel 1988 handelden leveranciers van beveiligingsoplossingen 1738 afzonderlijke bedreigingen af. In de eerste twee maanden van 2008 alleen al werden 1,1 miljoen afzonderlijke bedreigingen gemeld. Trend Micro heeft het aantal webbedreigingen sinds 2005 met 1731% zien toenemen.

Leveranciers van beveiligingsoplossingen spelen hier op in door vaker met patroonupdates te komen. Deze overweldigende toename van het aantal bedreigingen en het bijbehorende aantal updates heeft aanzienlijke gevolgen voor de systeembronnen die zijn vereist om deze patronen te downloaden, waardoor vaak kritieke prestatieproblemen ontstaan. Deze aanpak kan niet op de lange termijn worden gehandhaafd.

OPLOSSING

Het Trend Micro Smart Protection Network biedt beveiliging die slimmer is dan conventionele benaderingswijzen doordat de allernieuwste bedreigingen worden geblokkeerd voordat ze u bereiken. Het Trend Micro Smart Protection Network, dat gebruikmaakt van alle oplossingen en services van Trend Micro, combineert unieke "in-the-cloud"-technologieën met lichtere clients, waardoor een krachtigere beveiliging wordt geboden terwijl u minder afhankelijk wordt van tijdrovende downloads van handtekeningen.

Het Trend Micro Smart Protection Network biedt realtime "betere beveiliging samen" tegen alle typen bedreigingen, van schadelijke bestanden, spam, phishing en webbedreigingen tot DoS-aanvallen (Denial of Service), kwetsbare websiteplekken en zelfs gegevensverlies. Combinaties van activiteiten wordt gecorreleerd om te bepalen of zij schadelijk zijn. Dat komt doordat één enkele activiteit van een webbedreiging gevaarloos kan lijken, terwijl een aantal verschillende activiteiten gezamenlijk een schadelijk resultaat kunnen opleveren. Stop webbedreigingen voordat ze u bereiken. Beveiliging die nog weer slimmer is.

BELANGRIJKSTE ONDERDELEN

- Webreputatietechnologie
- E-mailreputatietechnologie
- Bestandsreputatietechnologie
- Correlatietechnologie met gedragsanalyse
- Feedbacklussen
- Kennis over bedreigingen (verzamelen en analyseren van bedreigingen)

BELANGRIJKSTE VOORDELEN

- Nieuwe bedreigingen, nieuwe afweer
- Sterkere, snellere bescherming met minder belasting van uw systeembronnen
- Beveiliging overal en altijd
- Meerlaagse bescherming
- Veelomvattende beveiliging
- Betere beveiliging samen
- Ondersteund door beproefd leiderschap en erkende deskundigheid op het gebied van contentbeveiliging

BELANGRIJKSTE ONDERDELEN

Webreputatie

Met een van de grootste reputatiedatabases voor domeinen ter wereld houdt de webreputatietechnologie van Trend Micro de geloofwaardigheid van webdomeinen bij door een reputatiescore toe te wijzen op basis van factoren zoals de leeftijd van een website, historische locatiewijzigingen en aanwijzingen voor verdachte activiteiten die naar boven komen uit de gedragsanalyse van malware.

E-mailreputatie

De e-mailreputatietechnologie van Trend Micro valideert IP-adressen door deze te controleren aan de hand van een reputatiedatabase van bekende spambronnen en door gebruik te maken van een dynamische service die de reputatie van de afzender van e-mail in realtime kan beoordelen. Reputatiescores worden verfijnd door middel van de onafgebroken analyse van het "gedrag", het activiteitenscala en de historische gegevens van IP-adressen. Schadelijke e-mailberichten worden "in-the-cloud" geblokkeerd op basis van het IP-adres van de afzender, waardoor bedreigingen het netwerk of de pc van de gebruiker niet meer kunnen bereiken.

Bestandsreputatie

Met "in-the-cloud" bestandsreputatietechnologie wordt de reputatie van elk bestand dat wordt gehost op een website of dat als bijlage aan een e-mailbericht is gehecht, gecontroleerd aan de hand van een uitgebreide database voordat een gebruiker toegang krijgt. Krachtige netwerken voor het afleveren van content en lokale cachingservers staan garant voor minimale vertraging. Aangezien de informatie over de malware "in-the-cloud" wordt opgeslagen, is deze onmiddellijk beschikbaar voor alle gebruikers op het netwerk.

Correlatie met gedragsanalyse

Met de correlatietechnologie met gedragsanalyse worden combinaties van activiteiten met elkaar in verband gebracht om te bepalen of deze schadelijk zijn. Eén enkele activiteit van een webbedreiging kan gevaarloos lijken, terwijl een aantal verschillende activiteiten gezamenlijk een schadelijk resultaat kunnen opleveren. Doordat de verschillende onderdelen van een bedreiging worden gecorreleerd en de bedreigingsdatabases onafgebroken worden bijgewerkt, kent Trend Micro het duidelijke voordeel van de response in realtime, waardoor onmiddellijk en automatisch bescherming kan worden geboden tegen e-mail- en webbedreigingen.

Feedbacklussen

Met geïntegreerde feedbacklussen wordt een onafgebroken communicatie verzorgd tussen Trend Micro producten en de centra en technologieën voor bedreigingsonderzoek van de onderneming die permanent actief zijn. Bij elke nieuwe bedreiging die wordt geïdentificeerd bij een standaard reputatiecontrole bij een klant worden alle bedreigingsdatabases van Trend Micro automatisch bijgewerkt waardoor de bedreiging bij elke volgende klant kan worden tegengehouden. Aangezien de bedreigingsgegevens worden verzameld op basis van de reputatie van de communicatiebron en niet van de inhoud van de specifieke communicatie, zijn de persoonlijke of zakelijke gegevens van een klant altijd beschermd.

Kennis over bedreigingen

Trend Micro is al 20 jaar leider op het gebied van de beveiliging van internetcontent en onderhoudt, verspreid over de wereld, datacenters op vijf locaties, waar elke dag meer dan 1,2 terabytes aan gegevens wordt verwerkt. TrendLabs™, het wereldwijde netwerk van onderzoeks-, service- en ondersteuningscentra van Trend Micro, zorgt voor een permanente bewaking tegen bedreigingen om aanvallen te voorkomen. Met meer dan 1000 beveiligingsdeskundigen wereldwijd en 24/7-beschikbaarheid biedt TrendLabs realtime tijdige beveiligingsmaatregelen voor het detecteren, anticiperen en elimineren van aanvallen.

Het Trend Micro Smart Protection Network verwerkt onafgebroken de kennis over bedreiging die wordt verzameld met behulp van het omvangrijke wereldwijde netwerk van honeypots, opgestuurde monsters, feedbacklussen, technologieën voor webcrawling, klanten, partners en TrendLabs-bedreigingsonderzoek zodat automatische, realtime bescherming tegen de allernieuwste bedreigingen kan worden geboden. De verzamelde bedreigingsgegevens worden in realtime geanalyseerd en gecorreleerd door middel van query's in de kennisbanken voor malware van Trend Micro en door TrendLabs.

Ga voor meer informatie naar <http://www.trendmicro.com/go/SmartProtectionNetwork>.



Copyright© 2008 Trend Micro Incorporated. Alle rechten voorbehouden. Trend Micro, het Trend Micro t-ball logo en TrendLabs zijn handelsmerken of gedeponeerde handelsmerken van Trend Micro, Incorporated. Alle overige product- of bedrijfsnamen zijn mogelijk handelsmerken of gedeponeerde handelsmerken van hun eigenaren. [DS01SPN_080624NL]

DE CIJFERS

- Trend Micro Smart Protection Network handelt dagelijks meer dan vijf miljard vragen af over URL's, e-mail en bestanden.
- Trend Micro verwerkt dagelijks meer dan 50 miljoen IP-adressen en URL's.
- Meer dan 250 miljoen ingestuurde monsters zijn afkomstig van het veelomvattende, wereldwijde systeem van Trend Micro van vallen, honeypots, product-feedbacklussen en andere beproefde verzameltechnieken.
- Verspreid over de wereld onderhoudt Trend Micro datacenters op vijf locaties, waar elke dag meer dan 1,2 terabytes aan gegevens wordt verwerkt.
- Bij Trend Micro werken meer dan 1000 beveiligingsdeskundigen die zorgen voor een onafgebroken bewaking tegen bedreigingen om aanvallen te voorkomen.
- Elke dag stopt Trend Micro 8 tot 10 miljoen infecties.