

Beveiliging van Internet

De performance van primaire processen bij financiële dienstverleners kan met Internet aanzienlijk worden verbeterd. Een veelgehoord argument om deze mogelijkheden nog niet te benutten is dat de techniek nog niet veilig genoeg zou zijn. Dit artikel behandelt een aantal bezwaren en laat zien welke mogelijkheden er bestaan om hieraan

Door drs. Henk ten Bos

Financiële dienstverleners kunnen hun productiviteit verdubbelen door een adequate toepassing van Internet in de primaire processen. Dit was te lezen in het artikel 'E-novation: nieuwe kans op performance-verbetering' uit het VVP van 21 april jl. De terugverdientijd van investeringen die voor een dergelijke forse productiviteitsstijging zorgen, ligt tussen de een en drie jaar. Vraag is dus waarom de financiële sector niet en masse de mogelijkheden van Internettoepassingen aangrijpt. Die aarzeling ligt vooral in de beveiliging van bedrijfskritische gegevens. Hiervoor is het noodzakelijk om systemen uit het eigen netwerk te koppelen aan het Internet. Dit geldt zowel voor de financiële dienstverlener, die informatie uit interne systemen via het Internet beschikbaar wil stellen, als ook voor het intermediair. Het intermediair zal immers, om optimaal gebruik te kunnen maken van de nieuwe mogelijkheden, er voor moeten zorgen dat de medewerkers op de werkplek toegang tot Internet hebben.

Koppeling

Op welke manier kan het eigen netwerk aan het Internet geknoopt worden? Het koppelen van het eigen bedrijfsnetwerk aan Internet is eenvoudig. Er is niet veel meer nodig dan een abonnement bij een provider, een ISDN-router en standaardsoftware. Na installatie en het configureren van de software vormt het bedrijfsnetwerk plotseling een onderdeel van het wereldwijde Internet. Uiteraard is dit voor de meeste bedrijven een ongewenste situatie: het is niet de bedoeling dat iedereen zomaar via het Internet toegang kan krijgen tot de eigen bedrijfssystemen. Om dit te voorkomen moet op het punt waar het netwerk gekoppeld is aan het Internet gebruik worden gemaakt van een firewall-constructie. Deze bestaat uit een computer met programmatuur die al het netwerkverkeer tussen het eigen netwerk en het Internet controleert op afzender en inhoud (denk aan computervirussen!). Alleen het verkeer dat expliciet is toegestaan van en naar het Internet wordt doorgelaten. Deze firewall zal bij de financiële instelling uiteraard andere functionaliteit hebben dan bij het intermediair. De eerste wil gegevens uit de eigen administratie beschikbaar stellen. De firewall zal daarom toestaan dat bepaalde systemen uit het eigen netwerk vanaf het Internet benaderd mogen worden. Andersom zal voor het intermediair gelden dat alleen eigen medewerkers vanaf de werkplek het Internet mogen gebruiken. Eigen systemen zijn dan vanaf het Internet in het geheel niet te benaderen.

*Henk ten Bos is als Senior Consultant werkzaam bij IG&H Management Consultants in Woerden op het gebied van Electronic Business. Hij is te bereiken via h.tenbos@igh.nl.

Voor zowel de firewall bij het intermediair als bij de financiële dienstverlener zijn tegenwoordig standaard oplossingen beschikbaar die gespecialiseerde bedrijven in korte tijd kunnen installeren.

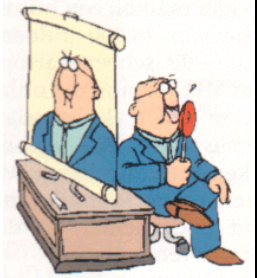
Afschermen

Hoe kan informatie op een veilige manier worden afgeschermd? Een informatieve website op het openbare Internet heeft vrijwel altijd tot doel om zoveel mogelijk bezoekers te trekken en toegang te bieden tot alle informatie die wordt aangeboden. Wanneer er informatie wordt aangeboden die specifiek voor één persoon bestemd is moeten extra maatregelen worden genomen. Een eenvoudige oplossing om informatie af te scherpen is gebruik te maken van een gebruikersnaam met wachtwoord. Per Internetpagina is aan te geven wie deze mag opvragen, waarbij ter controle eerst om een gebruikersnaam en wachtwoord wordt gevraagd. Op basis van de ingevoerde gegevens bepaalt de financiële instelling welke informatie zichtbaar is.

Autenticatie

Het gebruik van een gebruikersnaam en wachtwoord is voldoende voor het opvragen van informatie die niet privacy gevoelig is. Wanneer er ook transacties kunnen worden gedaan is het belangrijk om zeer te weten dat de transactie afkomstig is van de juiste persoon: de gebruiker op het Internet moet geauthenticeerd worden.

Veel manieren om een gebruiker te authenticeren maken gebruik van iets dat iemand in zijn/haar bezit moet hebben. Hierin ligt een uitdaging voor de financiële dienstverleners om te proberen tot een gezamenlijke oplossing te komen. Het intermediair zit uiteraard niet te wachten op een scala aan verschillende tokens en smartcards.



Beveiliging met alleen een gebruikersnaam en wachtwoord is in de meeste gevallen onvoldoende. De gegevens kunnen vrij eenvoudig in handen komen van een onbevoegd iemand. Zeker wanneer het mogelijk is om via de site van de financiële dienstverlener aanvragen of mutaties in te sturen zijn aanvullende maatregelen nodig.

Waar de eerstgenoemde manier van herkenning van de gebruiker nog gebaseerd is op wat iemand weet (een code), zijn veiliger methoden gebaseerd op iets dat iemand in zijn of haar bezit heeft.

Eén manier is het vooraf uitreiken van een *digitaal certificaat* dat op de computer wordt geïnstalleerd. Alléén met behulp van dit certificaat kan de informatie vanaf de Internetsite worden gelezen. Op het VerzekeringsAtrium is sinds enige tijd het Digitale Paspoot beschikbaar, dat gebruik maakt van deze methode.

Alhoewel een dergelijk certificaat een goede beveiliging biedt kleven er nadelen aan. Wanneer het intermediair een nieuwe computer aanschafft moet het certificaat opnieuw worden geïnstalleerd. Daarnaast is het certificaat eenvoudig via een diskette naar een andere computer te kopiëren.

Een aantal financiële instellingen gaat daarom nog een stap verder en maakt gebruik van *Tokens of smartcards*. Bij deze techniek, die bijvoorbeeld ook gebruikt wordt voor elektronisch bankieren, krijgt een klant een apparaatje. Voordat de informatie op het Internet wordt getoond verschijnt een code op het scherm die het intermediair op het apparaat moet intoetsen, waarna een andere code weer op het Internet moet worden ingevuld. Alleen met deze code is de informatie op te vragen. Tokens en smartcards bieden een uitstekende beveiliging, maar zijn in het algemeen erg kostbaar. Bovendien moet de gebruiker zorgvuldig omgaan met het apparaatje.

Encryptie-algoritme

De versleuteling die wordt gebruikt lijkt op de manier waarop kinderen 'geheime' boodschappen met elkaar uitwisselen.

Er wordt bijvoorbeeld afgesproken dat een bericht wordt opgeschreven in cijfers in plaats van letters waarbij A=1, B=2, C=3 enz. De ontvanger van het bericht moet dit encryptie-algoritme kennen om de originele boodschap te kunnen ontcijferen.

De in de praktijk gebruikte algoritmes zijn een stuk ingewikkelder, zodat het onmogelijk is ze binnen een bepaalde tijd te kraken.



Lezen

Omdat het Internet een "open" netwerk is, kan iedereen die over de benodigde kennis beschikt de informatie lezen die computers onderling uitwisselen. Uiteraard is dit niet de bedoeling en ook niet toegestaan wanneer we bijvoorbeeld naar de Wet Persoons Registratie kijken.

Onleesbaar maken van gegevens voor ze worden verstuurd (encryptie) biedt uitkomst. Hiervoor is een aantal methoden beschikbaar gebaseerd op het uitwisselen van sleutels. Alleen wie over een geheime sleutel beschikt, kan achter de originele inhoud van de berichten komen. Encryptie is tegenwoordig standaard opgenomen in de programmatuur die voor het Internet wordt gebruikt.

Technische maatregelen

Het nemen van maatregelen op het gebied van de techniek is noodzakelijk om een veilige verbinding met het Internet te maken, maar is niet voldoende. Constante monitoring en controle van de genomen maatregelen is nodig. De volgende punten zijn belangrijk:

1. *Logging en monitoring*. De activiteiten van de firewall en de Internetservers moeten in logbestanden worden bij

gehouden en periodiek worden gecontroleerd. Hierdoor is het mogelijk inbraakpogingen snel te detecteren.

2. *Procedures*. In richtlijnen staat beschreven hoe de beveiliging is ingericht, welke regels er zijn en hoe bepaalde taken uitgevoerd moeten worden. Zonder formele procedures bestaat het gevaar dat essentiële zaken er bij inschieten.

3. *Onderhoud en opleiding*. Beveiliging is een dynamisch proces en beheer van van de infrastructuur vereist een gedegen kennis van een beheerder. Deze kennis moet zich voortdurend vernieuwen vanwege de ontwikkelingen in de markt.

4. *Beveiligingsbewustzijn*. De noodzaak van beveiliging is niet alleen een zaak van de automatiseringsafdeling, maar is op ieder niveau in de organisatie een issue. Iedereen dient er bijvoorbeeld van bewust te zijn dat zorgvuldig met wachtwoorden moet worden omgegaan.

Mogelijkheden

Aandachtspunten bij beveiliging

1. *Fysieke beveiliging*

Firewall bij koppeling met Internet

2. *Autorisatie*

Gebruik gebruikersnaam en wachtwoord

3. *Authenticatie*

Extra controle op identiteit klant

4. *Encryptie*

Versleuteling gegevens

5. *Beheer*

Logging en monitoring, procedures, onderhoud en opleiding, beveiligingsbewustzijn



Internet-technologie biedt uitgelezen mogelijkheden om de performance van primaire processen te verbeteren. Verdubbeling van de productiviteit is een reële verwachting. Veel partijen aarzelen nog omdat ze de beveiliging van het Internet nog niet vertrouwen en niet altijd de organisatorische consequenties overzien.

Wanneer bij de realisatie gelet wordt op de technische en organisatorische aandachtspunten die hier zijn genoemd, dan is het Internet net zo veilig als de conventionele manier van zakendoen.