

PC-beveiliging

Karel Titeca

9 december 2004

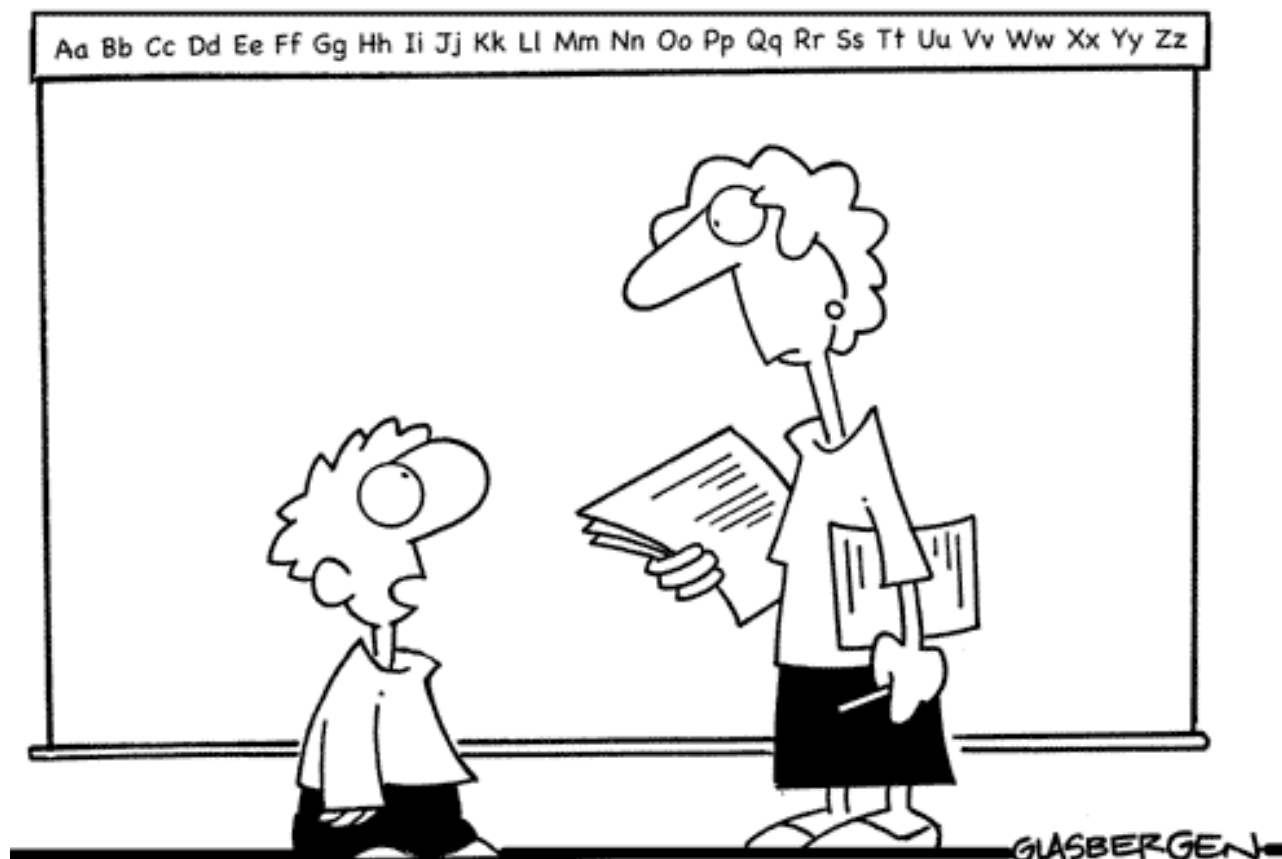


PC-beveiliging

- Inleiding
 - Wat zijn de problemen en gevaren?
 - Inleidende begrippen
- Wat kunt u doen?
 - Gebruik van wachtwoorden
 - Virusscanner
 - Windows Update
 - Spyware scanners
 - Personal firewalls
 - Bijkomende software
- Algemene tips



Beveiliging, een noodzaak



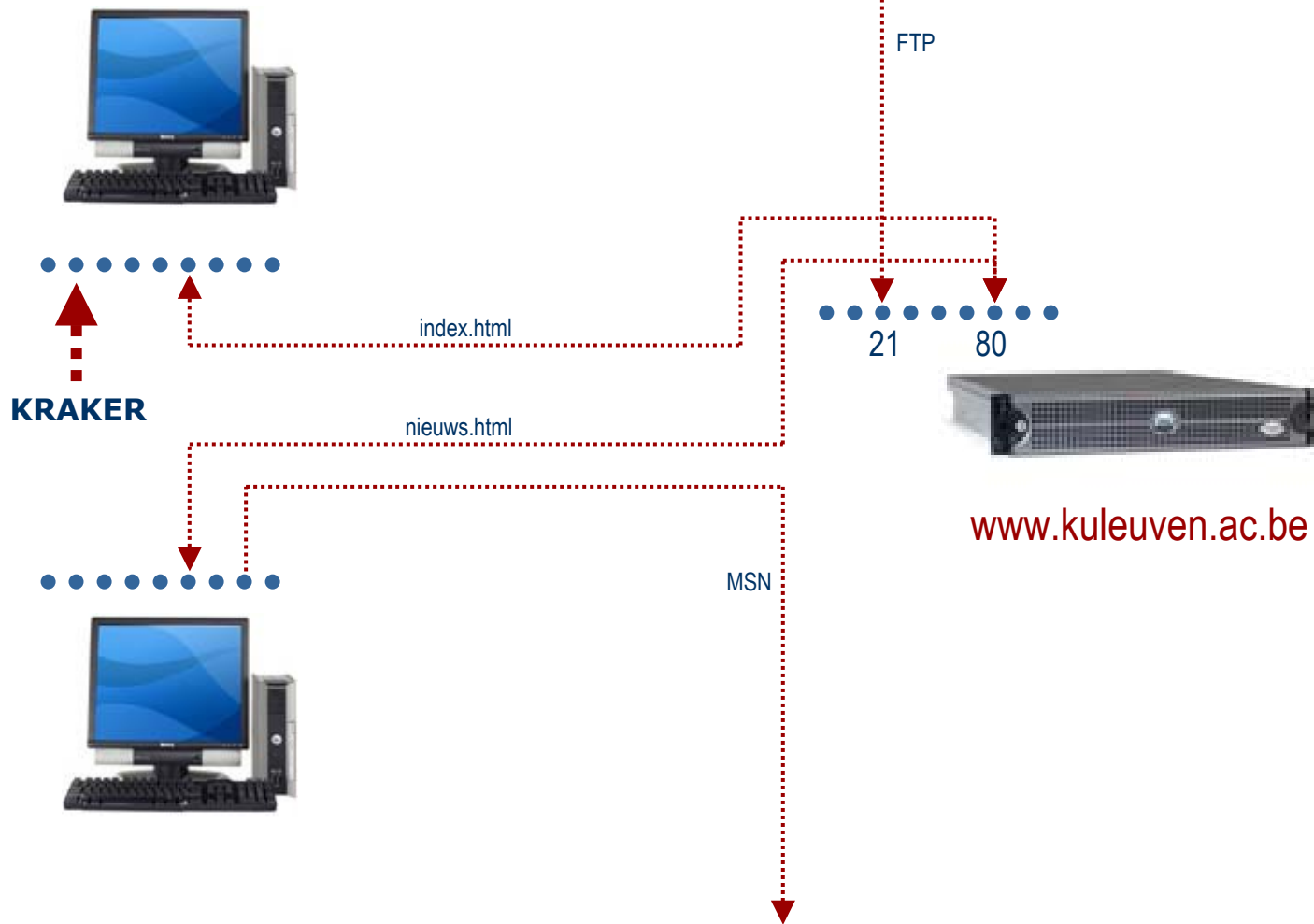
“Yes, I copied off Norman’s paper. Is it my fault if information security is lax around here?”

Inleiding

- Kabelverbinding = permanent online
- Permanent online = permanent kwetsbaar
- Kraker komt je PC binnen via beveiligingslek en neemt je PC over of kraakt andere PC's via jouw PC
- **We moeten zoveel mogelijk deuren (poorten) sluiten!**



Inleiding



Inleidende begrippen

■ Wat is een virus?

- Is een programma dat zich hecht aan andere programma's of bestanden
- Is zo gemaakt dat het zichzelf kan repliceren
- Probeert zich te verspreiden van computer naar computer
- Verspreiding kan enkel gebeuren door handelingen van de gebruiker (sturen van een e-mail, uitwisselen van bestanden, ...)
- Toegebrachte schade varieert van licht vervelende nevenwerkingen tot zuiver destructieve acties
- Kan schade berokkenen aan software of aan informatie in bestanden



Inleidende begrippen

■ Wat is een worm?

- Probeert zich te verspreiden van host naar host
- Heeft geen handelingen van de gebruiker nodig: kan zichzelf automatisch verspreiden
- Heeft ook geen andere bestanden nodig om zich aan te hechten: kan zich zelfstandig verspreiden
- Verspreiding gebeurt meestal aan de hand van e-mail-adressen die op de geïnfecteerde computer aangetroffen worden.
- Veroorzaakt meestal een toename in het netwerkverkeer, waardoor normale programma's langzamer gaan werken, in het slechtste geval soms volledig stilvallen
- Recent voorbeeld: de Sasser worm



Inleidende begrippen

■ Wat is een Trojaans paard?

- Lijkt op het eerste zicht een nuttig programma, veroorzaakt in werkelijkheid echter schade
- Meest voorkomende vormen van verspreiding:
 - als **attachment** via e-mail van een ogenschijnlijk betrouwbare bron (bv. "hier is een update voor Windows")
 - **genesteld** in software die je gratis kan downloaden



Inleidende begrippen

■ Wat is een **hoax**?

- Soms krijg je in je mailbox een waarschuwing voor een "nieuw virus"
- De mailberichten zijn bedoeld om je **schrik** aan te jagen:
 - Het is een héél gevaarlijk virus
 - Het wist onmiddellijk je harde schijf
 - Geen enkele virusscanner herkent het
 - Het is bevestigd door Microsoft of IBM of ...
- Vaak zijn dit **valse meldingen**, bedoeld om je vitale bestanden te laten verwijderen, of om een mailstroom te veroorzaken
- Stuur deze berichten niet zonder verifiëren of nadenken door!

Inleidende begrippen

■ Wat is spyware?

- Software die zich heimelijk op je PC nestelt
- Wordt vaak mee geïnstalleerd samen met andere software die je downloadt van internet
- Programmaatjes die in de achtergrond werken
- Verzamelen allerhande gegevens, gaande van websites die je bezoekt tot gebruikersnamen, wachtwoorden, credit card nummers, ...
- Laat soms reclamebanners verschijnen op je PC



Inleidende begrippen

- Spyware is meestal **belastend** voor het systeem
- De programma's hebben echter **geen destructieve werking** (zoals virussen)
- Vormen een **gevaar** voor de privacy



Inleidende begrippen

- **Keyloggers** houden je **toetsaanslagen** bij, en verzamelen zo gebruikersnamen en paswoorden
- **Browserkapers** nemen een stuk van je browser over, en installeren **ongewenste toolbars** of veranderen je thuispagina



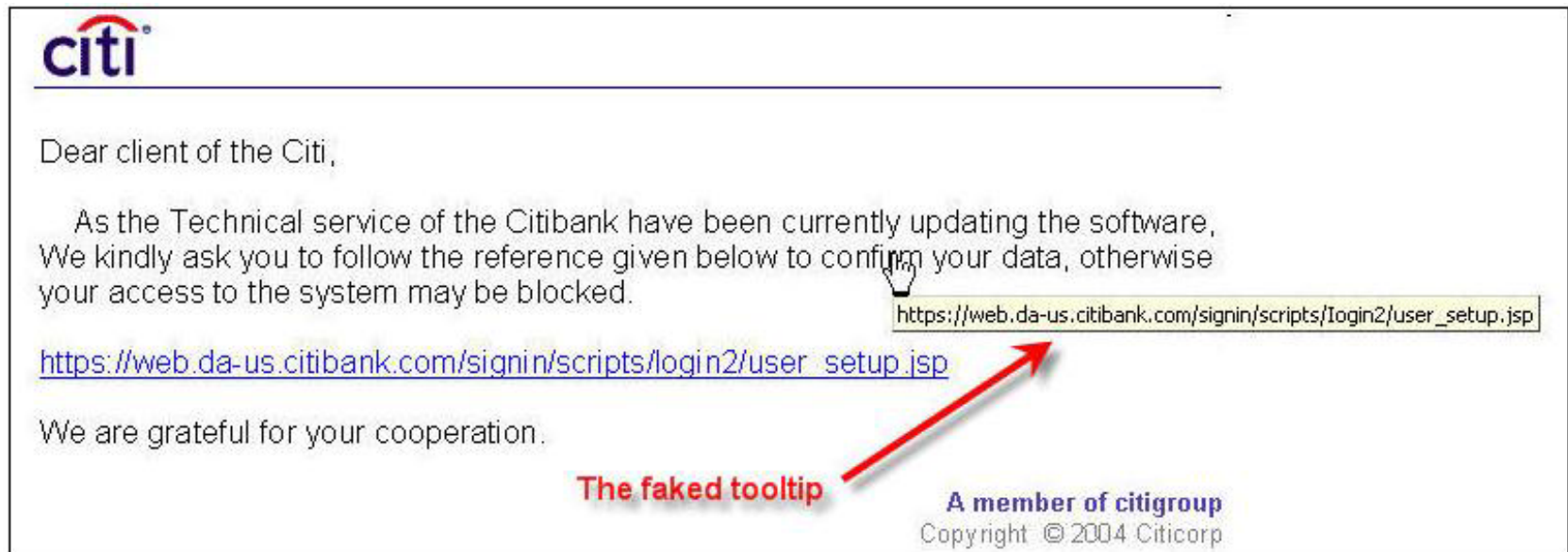
Inleidende begrippen

■ Wat is phishing?

- Phishing is een methode waarmee men probeert om allerhande **gevoelige informatie** (paswoorden, credit card nummers, ...) te ontfutselen van de gebruiker
- Gebeurt vaak aan de hand van een elektronisch **invulformulier**
- Gebruiker ontvangt een e-mail of wordt via een pop-up naar een site gelokt
- Afzenderadres is meestal **vervalst**
- E-mail is meestal in HTML
- Invulformulier **lijkt betrouwbaar** (pagina heeft bv. dezelfde opmaak als de pagina's van een of andere financiële instelling)

Inleidende begrippen

- Gebruiker wordt met een smoesje overhaald om zijn informatie in te vullen (bv. 'Gelieve uw gegevens te hernieuwen')



The screenshot shows a phishing email from Citi. The email body contains the following text:

citi

Dear client of the Citi,

As the Technical service of the Citibank have been currently updating the software, We kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.

https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp

We are grateful for your cooperation.

The faked tooltip (indicated by a red arrow) points to a tooltip that displays the URL: `https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp`.

A member of citigroup
Copyright © 2004 Citicorp

Inleidende begrippen



■ Wat zijn cookies?

- Cookies zijn **kleine tekstbestandjes** (max. 255 karakters) die door een website op uw computer aangemaakt worden
- Bevatten meestal **info** over de acties die je op die website ondernomen hebt, welke pagina's je bekeken hebt e.d.
- **Kunnen ook persoonlijke informatie bevatten** die je op die site opgegeven hebt
- Geplaatste cookies kunnen bij normaal surfen enkel terug opgevraagd worden door de site die de cookie geplaatst heeft.
- Websites kunnen ook derden toelaten om cookies op uw computer te plaatsen (bv. adverteerders op die website)
- Vele sites kunnen enkel optimaal gebruikt worden wanneer cookies toegelaten worden

Inleidende begrippen



■ Permanente vs. tijdelijke cookies

- **Permanente** cookies: blijven op uw computer wanneer de browser afgesloten wordt
- **Tijdelijke** cookies: worden verwijderd wanneer de browser afgesloten wordt. Deze cookies gelden enkel voor de lopende sessie

■ Directe vs. indirecte cookies

- **Directe** cookie: is gemaakt door, of wordt verzonden naar de website die je aan het bekijken bent
- **Indirecte** cookie: is gemaakt door, of wordt verzonden naar een andere website dan degene die je aan het bekijken bent (bv. adverteerder op pagina)

Inleidende begrippen



- Zijn cookies gevaarlijk?
 - Cookies verwijderen geen gegevens of beschadigen niets
 - Cookies kunnen geen virussen verspreiden; het zijn gewone tekstbestanden
 - Cookies vormen enkel een mogelijk gevaar voor de privacy; ze kunnen informatie bevatten over uw surfgedrag en mogelijk ook persoonlijke informatie

Inleidende begrippen

■ Wat is SPAM?



- Een zelfde mail die **ongevraagd** naar duizenden geadresseerden tegelijk wordt gestuurd
- Bevat meestal, maar niet noodzakelijk, **reclame**

Wat kan ik doen?

- Gebruik van wachtwoorden
- Virusscanner
- Windows Update
- Spyware scanners
- Persoonlijke firewalls
- Bijkomende software
- Wees altijd voorzichtig!



Wachtwoorden

- Scherm gevoelige informatie zoveel mogelijk af met een wachtwoord
- Gebruik verschillende wachtwoorden voor verschillende toepassingen
- Wijzig kritische wachtwoorden van tijd tot tijd
- Geef je wachtwoord enkel in op beveiligde webpagina's
- Schrijf je wachtwoord nergens op
- Gebruik enkel sterke wachtwoorden



Wachtwoorden

■ Wat zijn sterke wachtwoorden?

- minimaal 7 tekens
- bevat
 - zowel hoofdletters [A-Z]
 - als kleine letters [a-z]
 - als cijfers [0-9]
 - als symbolen ~!@#\$%^&*()_+ -= { } | [] \ : " ; ' < > ? , . /
- uw naam of namen van familieleden of huisdieren komen niet voor in het wachtwoord
- het wachtwoord is geen gewoon woord



Wachtwoorden

- Hoe worden wachtwoorden gekraakt?
 - Men probeert het wachtwoord op een of andere manier te raden
 - Men probeert één voor één alle woorden uit een woordenlijst (bv. woordenboek)
 - Men genereert alle mogelijke combinaties van tekens

- Een sterk wachtwoord is enkel te kraken volgens methode 3



Wachtwoorden

- Hoe onthoud ik een sterk wachtwoord?
 - Neem een makkelijk te onthouden, betekenisvolle zin
bv. "Shrubberies are my trade – I am a shrubber"
 - Neem van elk woord telkens de eerste letter
bv. "samtiaas"
 - Vervang bv. de i's door 1'en en de o's door 0'en
bv. "samt1aas"
 - Voeg symbolen en hoofdletters toe
bv. "saMt_1aAs"



Virusscanners



- Een virusscanner beschermt ons tegen virussen, trojaanse paarden en wormen
- Een virusscanner doet twee zaken:
 - **On-demand scan**: scannen van de harde schijf of een bepaalde map, op verzoek
 - **On-access scan**: bestanden die gebruikt worden scannen voor gebruik (op de achtergrond)
- Personeel en studenten van de K.U.Leuven mogen gebruik maken van Total Virus Defense

Virusscanners

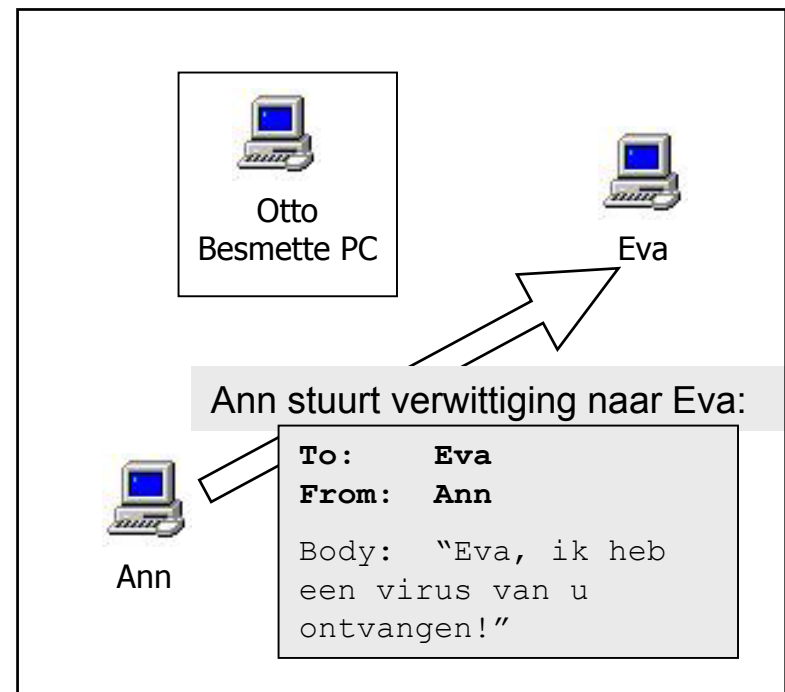
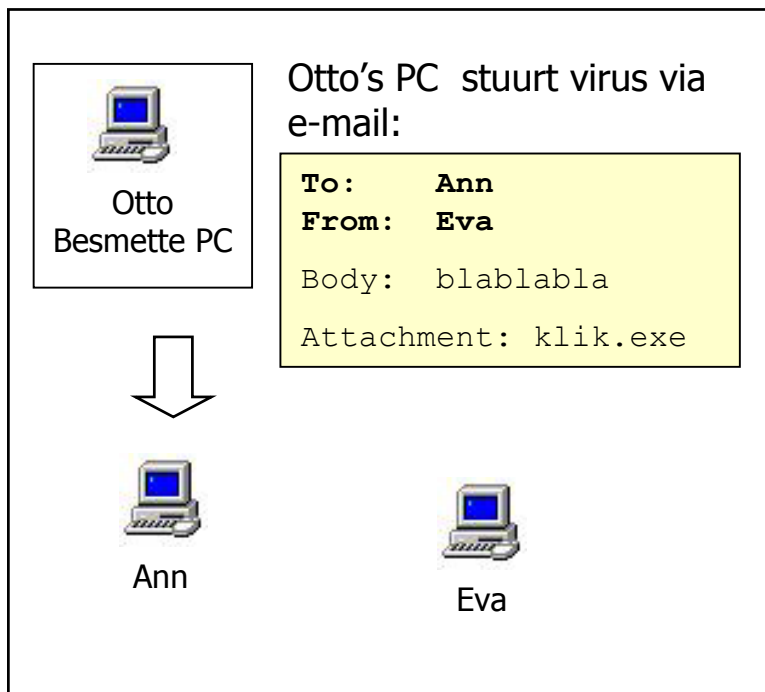


- Hou je virusscanner **up to date!**
- LUDIT scant mail centraal op virussen
- **Blijf voorzichtig!**
 - Open nooit een attachment van een vreemde
 - Open geen attachments van kennissen indien de mail onverwacht komt en de inhoud vreemd lijkt



Virusscanners

- "Ik krijg mails dat mijn PC een virus verstuurd heeft"
 - Veel virussen sturen mails naar willekeurige mail-adressen, met een willekeurig afzendadres
 - Verwittigingen terugsturen naar de ogenschijnlijke afzender heeft dus dikwijls geen zin



Windows update



- Er worden regelmatig fouten (bugs) ontdekt in software
- Een veiligheidslek wordt gedicht met een patch
- Microsoft verdeelt patches voor zijn producten via de Windows Update
<http://windowsupdate.microsoft.com>

Windows update



- Er zijn 3 soorten updates
 - Kritische (high priority) updates
 - Optionele software updates
 - Optionele hardware updates

- De kritische updates moeten zo snel mogelijk geïnstalleerd worden!

- Updaten kan geautomatiseerd worden

Spyware scanners

- Virusscanners controleren enkel op virussen, wormen en trojaanse paarden
 - Voor spyware zijn er aparte scan-producten
 - Scannen meestal niet op achtergrond
 - Ook hier: [updates noodzakelijk!](#)
-
- **Ad-Aware SE**
 - **SpyBot Search & Destroy**



Persoonlijke firewalls



**“I know a lot of highly-confidential company secrets,
so my boss made me get a firewall installed.”**

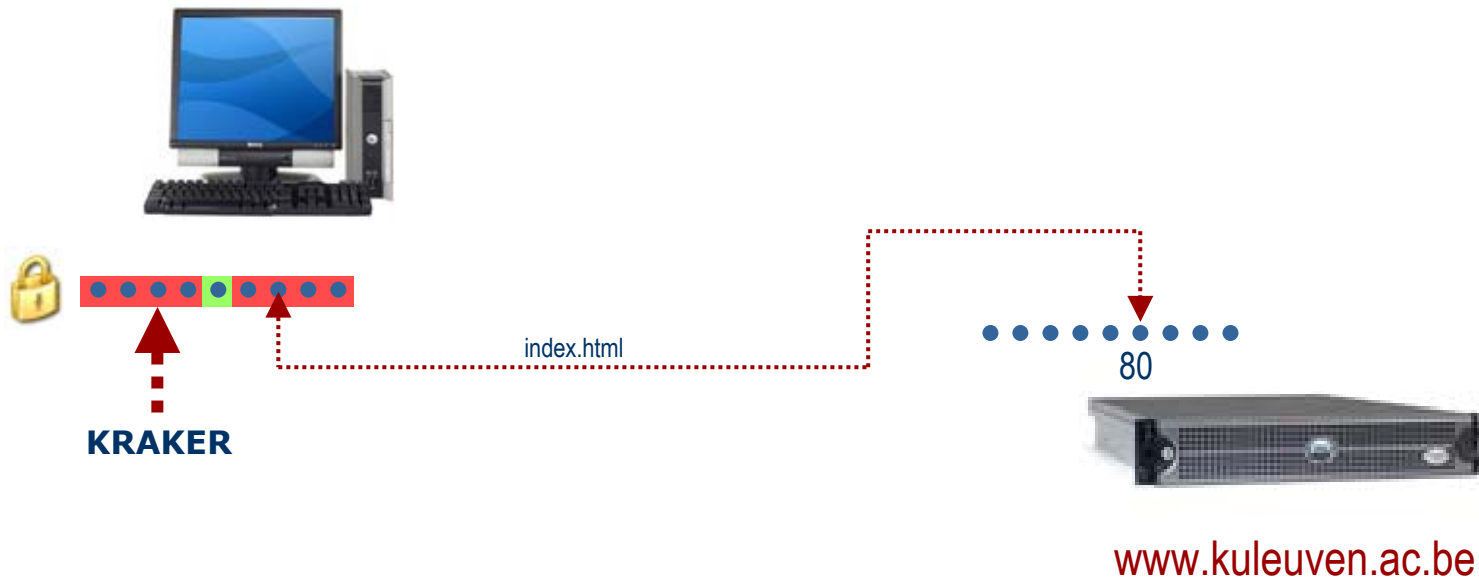
Persoonlijke firewalls

■ Hoe breekt iemand in mijn PC in?



- iemand laat je een **onbetrouwbaar** programma uitvoeren (per mail, per MSN, ...)
- iemand voert een **'portscan'** uit
- iemand opent een gedeelde Windows-map waar **geen wachtwoord** voor geconfigureerd is
- een programma bevat een **beveiligingsfout** waarlangs een inbreker binnen kan
- een programma is **slecht geconfigureerd**
- een programma is **slecht gemaakt**

Persoonlijke firewalls



Persoonlijke firewalls

- Firewalls **blokkeren** de toegang tot onze computer
 - van buiten naar binnen
 - van binnen naar buiten
- Een firewall **detecteert** inbraakpogingen
- Een firewall **leert** gaandeweg

- **ZoneLabs ZoneAlarm**
- **Kerio Personal Firewall**
- **Windows Firewall**



SPAM



■ Hoe komt men aan mijn mailadres?

- Automatisch scannen van webpagina's op zoek naar e-mail-adressen
- Automatisch scannen van nieuwsgroepen naar e-mail-adressen
- Gebruikers proberen te lokken naar een webpagina waar men het mailadres moet invullen
- 'Raden' van mailadressen: info@..., contact@..., ...
- Forwards van forwards van forwards
- Sites die lijsten van mailadressen verkopen
- ...

SPAM



■ Wat kan ik ertegen doen?

- Wees voorzichtig met het uitdelen van uw mail-adres
- Neem een speciale mail-account bij een gratis provider voor het invullen van online formulieren
- Gebruik een dienst als Mailinator
- Deel uw hoofdadres enkel met personen die je vertrouwt

SPAM



■ Wat kan ik ertegen doen?

- Wanneer je op nieuwsgroepen of fora post, gebruik dan een vervormd mailadres, bv. karel@DOEWEG.kuleuven.be ipv karel@kuleuven.be
- Plaats uw mailadres zo weinig mogelijk op webpagina's
- Gebruik het BCC-veld bij e-mails
- Reageer nooit op SPAM
- Bekijk uw mails zonder afbeeldingen

SPAM

- K.U.Leuven markeert mails met een hoge SPAM-score als [SPAM?]
- Filtering in mailprogramma
- Mailprogramma met Junk Mail-mogelijkheden



Mozilla Thunderbird

Bijkomende software



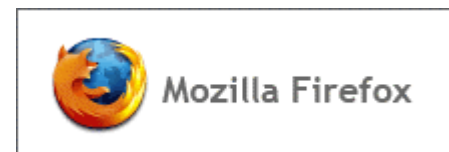
■ Mailsoftware en webmail

- junk mail mogelijkheden
- geen externe afbeeldingen
- geen automatische previews
- geen automatische uitvoering van attachments
- HTML vs. plain text

Bijkomende software

■ Browser en toebehoren

- geen beveiligingslekken
- cookie-instellingen
- pop-up-blocker (Google toolbar)
- geen automatische uitvoering van onveilige programma's



Algemene tips

- Let **altijd** op met e-mail-attachments
- Installeer een **virusscanner**
- Installeer een **persoonlijke firewall**
- Installeer de **laatste updates** voor uw software
- Gebruik enkel **betrouwbare software**
- Controleer uw systeem geregeld op **spyware**



Algemene tips

- Gebruik wachtwoorden, **veilige wachtwoorden**
- **Reageer nooit op mails** die vragen naar persoonlijke of financiële informatie
- **Geef nooit een wachtwoord door per e-mail**
- Vul gevoelige informatie enkel in op een **beveiligde webpagina**
- **Blijf kritisch**



Vragen? Meer info?



Karel Titeca
K.U.Leuven • LUDIT

W. de Croylaan 52a • Heverlee

karel.titeca@DOEWEG.cc.kuleuven.ac.be

<http://ludit.kuleuven.be/software/beveiliging>