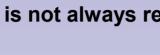


What you feel is not always real

The Windchill Factor

"Cloudburst" (Rock Song, 1994)





Copyright Information



Some rights reserved / Einige Rechte vorbehalten

Michael Kafka, René Pfeiffer, Vienna, Austria

You may freely use, distribute and modify this work under following agreement:

Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:



Authors must be referenced (also for modification) Autoren müssen genannt werden (auch bei Bearbeitung)



Only for non commercial use Nur für nichtkommerzielle Nutzung



Creative

Derivative work under same licence Derivative Arbeit unter selber Lizenz

http://www.creativecommons.com



Trust, Belief, Fear, Doubt

Agenda Blind Trust Simplified Security FUD and Panic The Unknown

The Windchill Factor

nterhaching 2010 yers of Insecurity

I have a firewall The products must be safe

Blind Trust





Trust the Product



The Vendor must implement security You get what you pay for. Product evaluation? Software Cheap, secure, fast – pick any two. There must be some "warranty" Terms of use!

I Have Firewall (Nothing can happen to me)

Understand "Firewall" Many functions Not all are implemented Have a plan What to defend against What to protect Which functions to use **Evaluate:** Which Product/Implementation fits



I Have an Antivirus Solution



They have to detect everything But:

Detection rate is dropping Evolution of malware speeds up Zero-Days proliferate AV filter use default *accept* policy

My Proxy protects me



Proxies will also proxy attacks Complexer than network filters Cannot see all malicious content Can act as *tunnel* proxy

The Browser Tells Me that I'm Safe

Trust model of Certificates Attacks on Certificates Phishing and Spoofing

Most browsers load and execute untrusted code



The Windchill Factor

nterhaching 2010 yers of Insecurity

Simplified Security

Click here to be safe One size fits all

"Everything should be made as simple as possible, but not simpler."

Albert Einstein









Security settings hide details Trust in the vendor Single-click-security is an illusion

Misunderstanding



The web site is encrypted. My VPN encrypts, therefore I am safe. It's only a text document. Audio/video is not executable.

FUD (Fear, Uncertainty and Doubt)



Spread fear, sell products.

"When he reached the New World, Cortez burned his ships. As a result his men were well motivated."

Captain Ramius, (The Hunt for Red October)



The Huns are Coming!

Press and Vendors:

Exaggerate Spread panic Want to sell their product Suppress independent research

Spread the bad news



Media coverage of attacks Worm/virus/trojan spread Hacking attacks! Google is down! Billions of \$ of damage! Distorted view of the "facts" No basis for sane decisions Reality is different

Historic Marketing



Method used to be common Create needs & enemies Offer remedies right thereafter

The Unknown (Or: "Surprise Surprise")



What the eye doesn't see, the heart doesn't grieve over.

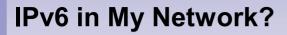
The world changes every day.

"Your current safe boundaries were once unknown frontiers."

Author Unknown



Unterhaching 2010 7 Layers of Insecurity





Yes it's (most likely) there! Apple OS-X Windows Vista Windows 7

Teredo



Pre-Configured? Where do want to tunnel today? Sans Institute: High rate of Teredo-Connections

Services, Ports & Protocols

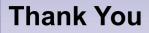


Poorly documented products Services? Protocols needed? Undocumented interactions Application - Application

The Cloud

Where is my data? Who processes my data? Can I still do audits? My virtual machine is my castle?





Questions?



Unterhaching 2010 7 Layers of Insecurity

