T&A SYSTEME

Sicher mit Microsoft!

Inhalt

T&A SYSTEME, Kurzvorstellung 1

Referent • Unternehmen

Sicher mit Microsoft? 2

Imagewechsel • Zahlen und Fakten

Security-Produkte 3

Frei Haus • Forefront

Sicher mit Microsoft! 4

Argumente

www.systeme.de

Sebastian Krück

Dipl.-Ing. Sebastian Krück

Consulting

sebastian.krueck@systeme.de

+49 2324 9258 534

+49 172 286 75 15

Consultant bei T&A SYSTEME

Schwerpunkte: Security Projekte, Microsoft Forefront, Security Technologien

Diplom Ingenieur für Sicherheit in der Informationstechnik

Ruhr Universität Bochum, Studium „Sicherheit in der Informationstechnik“

Über uns: Steckbrief

Typ:	Dienstleister / Systemintegrator im Bereich IT-Infrastrukturen
Gründung:	Dezember 1994
Größe:	55 Mitarbeiter EUR 8,8 Mio. Umsatz p.a.
RZ-Power:	Eigenes Rechenzentrum für ca. 500 Server, abgesichert und mit 40 TB SAN-Kapazität. Full-Managed Betrieb ist möglich.
Kunden:	Nationale & internationale Unternehmen in unterschiedlichen Branchen
Leitsatz:	„Keep IT simple“

Sicher mit Microsoft?

Microsoft
Windows xp with Firewall

Imagewechsel

- E-Mail von Bill Gates an alle MS-Mitarbeiter (Januar 2002)

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing – or able – to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing. When we started work on Microsoft .NET more than two years ago, we set a new direction for the company – and articulated a new way to think about our software. Rather than developing standalone applications and Web sites, today we're moving towards smart clients with rich user interfaces interacting with Web services. We're driving the XML Web services standards so that systems from all vendors can share information, while working to make Windows the best client and server for this new era.

There is a lot of excitement about what this architecture makes possible. It allows the dreams about e-business that have been hyped over the last few years to become a reality. It enables people to collaborate in new ways, including how they read, communicate, share annotations, analyze information and meet.

However, even more important than any of these new capabilities is the fact that it is designed from the ground up to deliver Trustworthy Computing. What I mean by this is that customers will always be able to rely on these systems to be available and to secure their information. Trustworthy Computing is computing that is as available, reliable and secure as electricity, water services and telephony.

Today, in the developed world, we do not worry about electricity and water services being available. With telephony, we rely both on its availability and its security for conducting highly confidential business transactions without worrying that information about who we call or what we say will be compromised. Computing falls well short of this, ranging from the individual user who isn't willing to add a new application because it might destabilize their system, to a corporation that moves slowly to embrace e-business because today's platforms don't make the grade.

The events of last year – from September's terrorist attacks to a number of malicious and highly publicized computer viruses – reminded every one of us how important it is to ensure the integrity and security of our critical infrastructure, whether it's the airlines or computer systems.

Computing is already an important part of many people's lives. Within ten years, it will be an integral and indispensable part of almost everything we do. Microsoft and the computer industry will only succeed in that world if CIOs, consumers and everyone else sees that Microsoft has created a platform for Trustworthy Computing.

Every week there are reports of newly discovered security problems in all kinds of software, from individual applications and services to Windows, Linux, Unix and other platforms. We have done a great job of having teams work around the clock to deliver security fixes for any problems that arise. Our responsiveness has been unmatched – but as an industry leader we can and must do better. Our new design approaches need to dramatically reduce the number of such issues that come up in the software that Microsoft, its partners and its customers create. We need to make it automatic for customers to get the benefits of these fixes. Eventually, our software should be so fundamentally secure that customers never even worry about it.

No Trustworthy Computing platform exists today. It is only in the context of the basic redesign we have done around .NET that we can achieve this. The key design decisions we made around .NET include the advances we need to deliver on this vision. Visual Studio .NET is the first multi-language tool that is optimized for the creation of secure code, so it is a key foundation element.

I've spent the past few months working with Craig Mundie's group and others across the company to define what achieving Trustworthy Computing will entail, and to focus our efforts on building trust into every one of our products and services. Key aspects include:

Availability: Our products should always be available when our customers need them. System outages should become a thing of the past because of a software architecture that supports redundancy and automatic recovery. Self-management should allow for service resumption without user intervention in almost every case.

Security: The data our software and services store on behalf of our customers should be protected from harm and used or modified only in appropriate ways. Security models should be easy for developers to understand and build into their applications.

Privacy: Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It should be easy for users to specify appropriate use of their information including controlling the use of email they send.

Trustworthiness is a much broader concept than security, and winning our customers' trust involves more than just fixing bugs and achieving "five-nines" availability. It's a fundamental challenge that spans the entire computing ecosystem, from individual chips all the way to global Internet services. It's about smart software, services and industry-wide cooperation.

There are many changes Microsoft needs to make as a company to ensure and keep our customers' trust at every level – from the way we develop software, to our support efforts, to our operational and business practices. As software has become ever more complex, interdependent and interconnected, our reputation as a company has in turn become more vulnerable. Flaws in a single Microsoft product, service or policy not only affect the quality of our platform and services overall, but also our customers' view of us as a company.

In recent months, we've stepped up programs and services that help us create better software and increase security for our customers. Last fall, we launched the Strategic Technology Protection Program, making software like IIS and Windows .NET Server secure by default, and educating our customers on how to get – and stay – secure. The error-reporting features built into Office XP and Windows XP are giving us a clear view of how to raise the level of reliability. The Office team is focused on training and processes that will anticipate and prevent security problems. In December, the Visual Studio .NET team conducted a comprehensive review of every aspect of their product for potential security issues. We will be conducting similarly intensive reviews in the Windows division and throughout the company in the coming months.

At the same time, we're in the process of training all our developers in the latest secure coding techniques. We've also published books like "Writing Secure Code," by Michael Howard and David LeBlanc, which gives all developers the tools they need to build secure software from the ground up. In addition, we must have even more highly trained sales, service and support people, along with offerings such as security assessments and broad security solutions. I encourage everyone at Microsoft to look at what we've done so far and think about how they can contribute.

But we need to go much further.

In the past, we've made our software and services more compelling for users by adding new features and functionality, and by making our platform richly extensible. We've done a terrific job at that, but all those great features won't matter unless customers trust our software. So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve. A good example of this is the changes we made in Outlook to avoid email borne viruses. If we discover a risk that a feature could compromise someone's privacy, that problem gets solved first. If there is any way we can better protect important data and minimize downtime, we should focus on this. These principles should apply at every stage of the development cycle of every kind of software we create, from operating systems and desktop applications to global Web services.

Going forward, we must develop technologies and policies that help businesses better manage ever larger networks of PCs, servers and other intelligent devices, knowing that their critical business systems are safe from harm. Systems will have to become self-managing and inherently resilient. We need to prepare now for the kind of software that will make this happen, and we must be the kind of company that people can rely on to deliver it.

This priority touches on all the software work we do. By delivering on Trustworthy Computing, customers will get dramatically more value out of our advances than they have in the past. The challenge here is one that Microsoft is uniquely suited to solve.

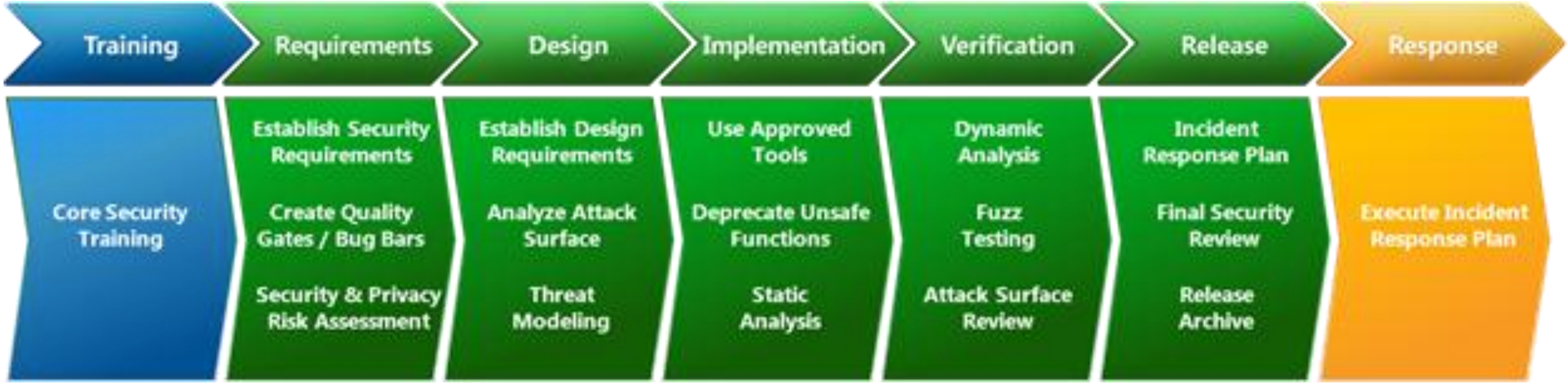
Bill

Imagewechsel

- “Trustworthy Computing is the highest priority for all the work we are doing.“
- “We must lead the industry to a whole new level of Trustworthiness in computing.”
- “So now, when we face a choice between adding features and resolving security issues, we need to choose security.”
- “Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve.”

Imagewechsel

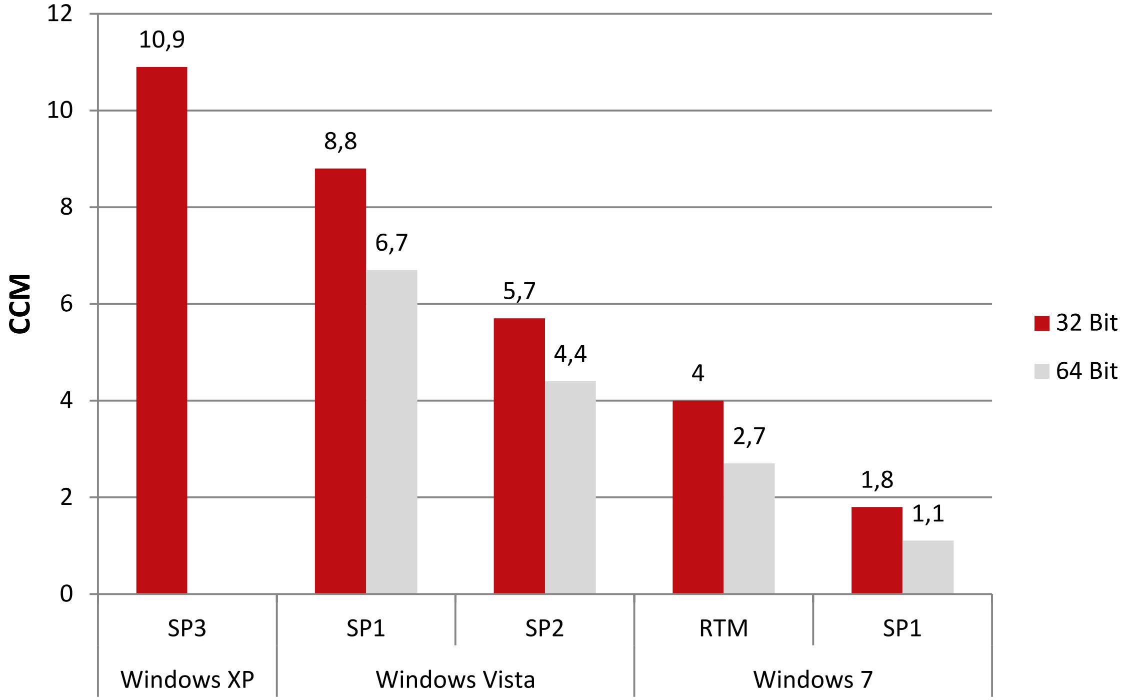
- Security Development Lifecycle

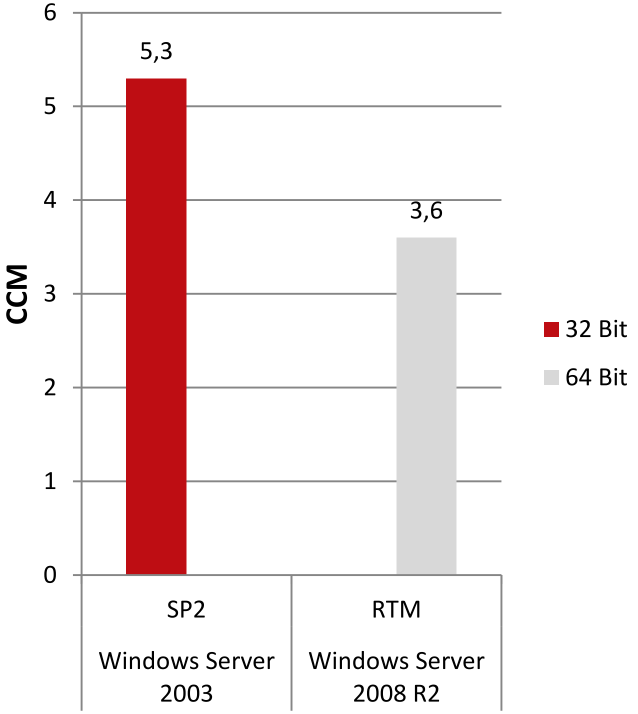


- „Checkliste“ zur sicheren Produktentwicklung (ca. 700 Punkte)
- Verpflichtend seit 2004
  - Windows Vista
  - 300 Produkte pro Jahr
    - Windows Patch, Serverbetriebssystem, Xbox-Spiele, …

Imagewechsel

- Sicherheit der Betriebssysteme:



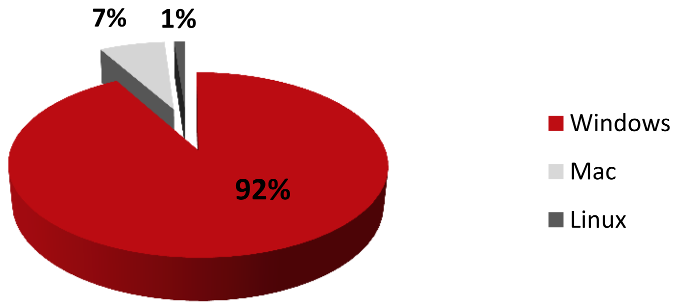


- Durchschnittliche vierteljährliche Infizierungsrate per CCM pro Betriebssystem und Service Pack für das Jahr 2010 (CCM = computers cleaned per mille (thousand))

Quelle: Microsoft Security Intelligence Report Ausgabe 11 (1. Halbjahr 2011)

Kein Weg vorbei an Microsoft

Weltweiter Marktanteil Betriebssystem

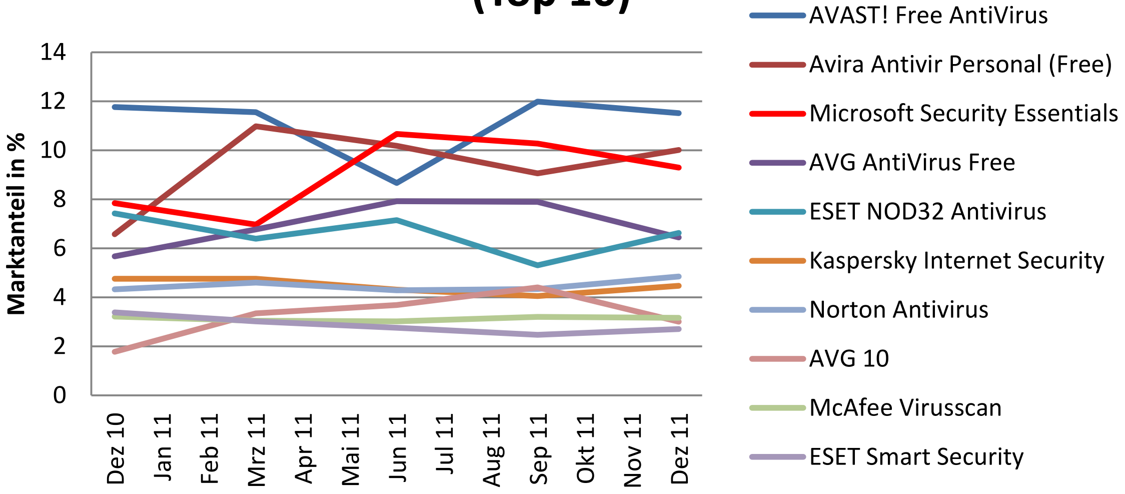


Quelle: netmarketshare.com 12.03.2012

Groupware-Marktführerschaft:
→ 65% Marktanteil für Microsoft Exchange in 2011

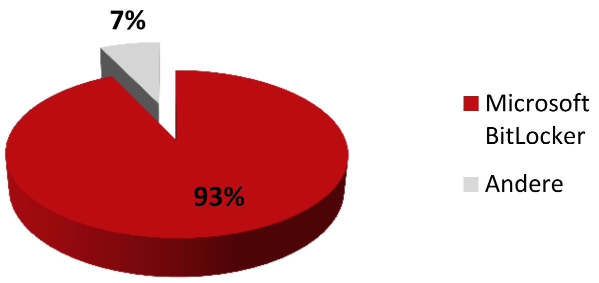
Quelle: Techconsult-Studie 2011

Weltweite Marktanteile Anti-Virus Software (Top 10)



Quelle: Opswat Security Industry Market Share Analysis 2010 /2011

Weltweiter Marktanteil Festplattenverschlüsselung



Quelle: Opswat Security Industry Market Share Analysis 2011

Sicherheit frei Haus

- Spy- und Malware-Erkennung
- Automatisch installiert und aktiviert
- Erweiterung zum Virenscanner unter Windows 8

- Datei- und Partitionsverschlüsselung

BitLocker

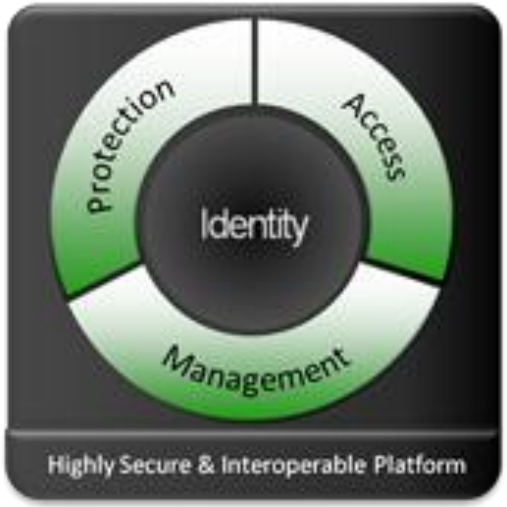
- Vollwertiger Virenscanner
- Microsoft Malware Engine
- Auch für Unternehmen bis 10 PCs

AppLocker

- Ausführen genehmigter Software
- Blockieren unerwünschter Software
- Unternehmensrichtlinien umsetzen

Business Ready Security

- Protection
  - Forefront Protection für Exchange Server / SharePoint
  - Forefront Endpoint Protection / SystemCenter Endpoint Protection
  - Forefront Online Protection für Exchange
- Access
  - Forefront Threat Management Gateway
  - Forefront Unified Access Gateway
- Management
  - System Center Configuration Manager
  - Forefront Protection Server Management Console
- Identity
  - Forefront Identity Manager



DirectAccess

Always On ohne VPN

Infrastructure Tunnel

- Zugriff auf Management Server
- Bidirektionale Verwaltung der Clients
  - Updates, Patches, GPOs,…

Intranet Tunnel

- Zugriff auf alle Ressourcen
- Arbeiten „wie intern“

Vollständige Integration ins Betriebssystem

Zugriff von jedem Standort

Volle Client-Kontrolle, auch bei längerer Abwesenheit

Überwachung der „Gesundheit“ durch Network Access Protection

T&A SYSTEME

Sicher mit Microsoft!

- Software und Schutz konsolidiert von einem Hersteller
  - Kenntnis der eigenen Technik → hohe Kompatibilität, tiefer Einblick in Kommunikation, vereinfachte Administration

- Integration führender Dritt-Hersteller in Microsoft Produkte
  - z.B. Anti-Virus Engines, Cloudmark Authority Engine

- Hohe Usability und vereinfachte Konfiguration
  - DirectAccess, „1-Klick-Aktivierung“, Templates

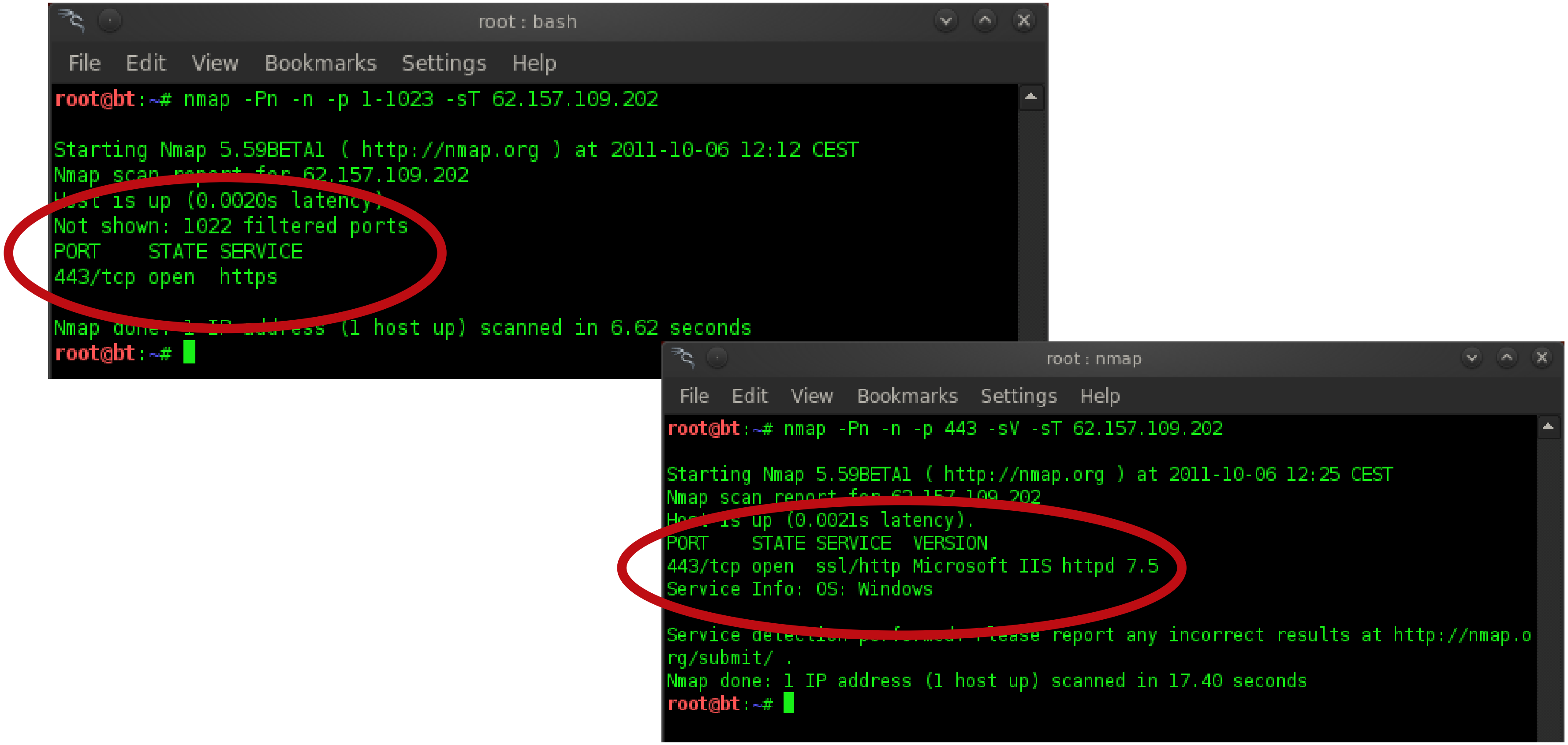
- Common Criteria Zertifizierung
  - Threat Management Gateway und Unified Access Gateway

Im Preis enthalten …

	Enterprise CAL Suite					
	Core CAL Suite					
Netzwerk-Infrastruktur		Windows Server			Windows RMS	
Zusammen-arbeit	Lync Standard	SharePoint Standard	Exchange Standard	Lync Enterprise	SharePoint Enterprise	Exchange Enterprise
Verwaltung		SCCM CML			SC Client Management	
Security		Forefront Endpoint Protection		Forefront Protection Suite	Unified Access Gateway	

Zum Angriff …

- Penetration Testing TMG und UAG
  - Portscan (Full connect, XMAS-Scan, …), OS detection, application mapping, webserver fingerprinting, …



root : bash
File Edit View Bookmarks Settings Help

```
root@bt:~# nmap -Pn -n -p 1-1023 -sT 62.157.109.202

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-10-06 12:12 CEST
Nmap scan report for 62.157.109.202
Host is up (0.0020s latency).
Not shown: 1022 filtered ports
PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds
root@bt:~# 
```

root : nmap
File Edit View Bookmarks Settings Help

```
root@bt:~# nmap -Pn -n -p 443 -sV -sT 62.157.109.202

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-10-06 12:25 CEST
Nmap scan report for 62.157.109.202
Host is up (0.0021s latency).
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Microsoft IIS httpd 7.5
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.40 seconds
root@bt:~# 
```

Zusammenfassung

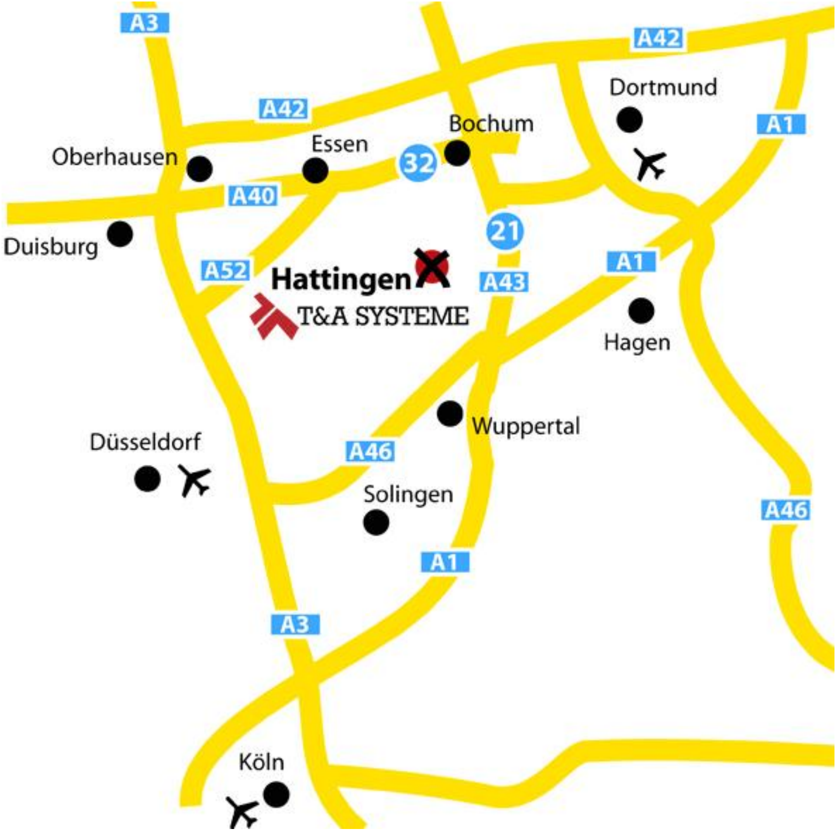
- **10 Jahre Trustworthy Computing Initiative**

- Große Fortschritte
  - Verbesserung der grundsätzlichen Produkt-Sicherheit
  - Hohe Integration und Kompatibilität
  - Hohe und verlässliche Sicherheit der Forefront Produkte

- Weiteres Verbesserungs-Potential
  - Reaktionszeit auf Sicherheitslücken
  - Microsoft Anti-Malware Engine

- **Sicher mit Microsoft!**

Kontaktdaten



T&A SYSTEME GmbH

Am Walzwerk 1
45527 Hattingen

+49 2324 9258 0

www.systeme.de
www.huettentalk.de

→ **Und hier am Messestand!**