

Schwachstellen auf Endgeräten Vom Besucher zum lokalen Admin

Andreas Bröhl

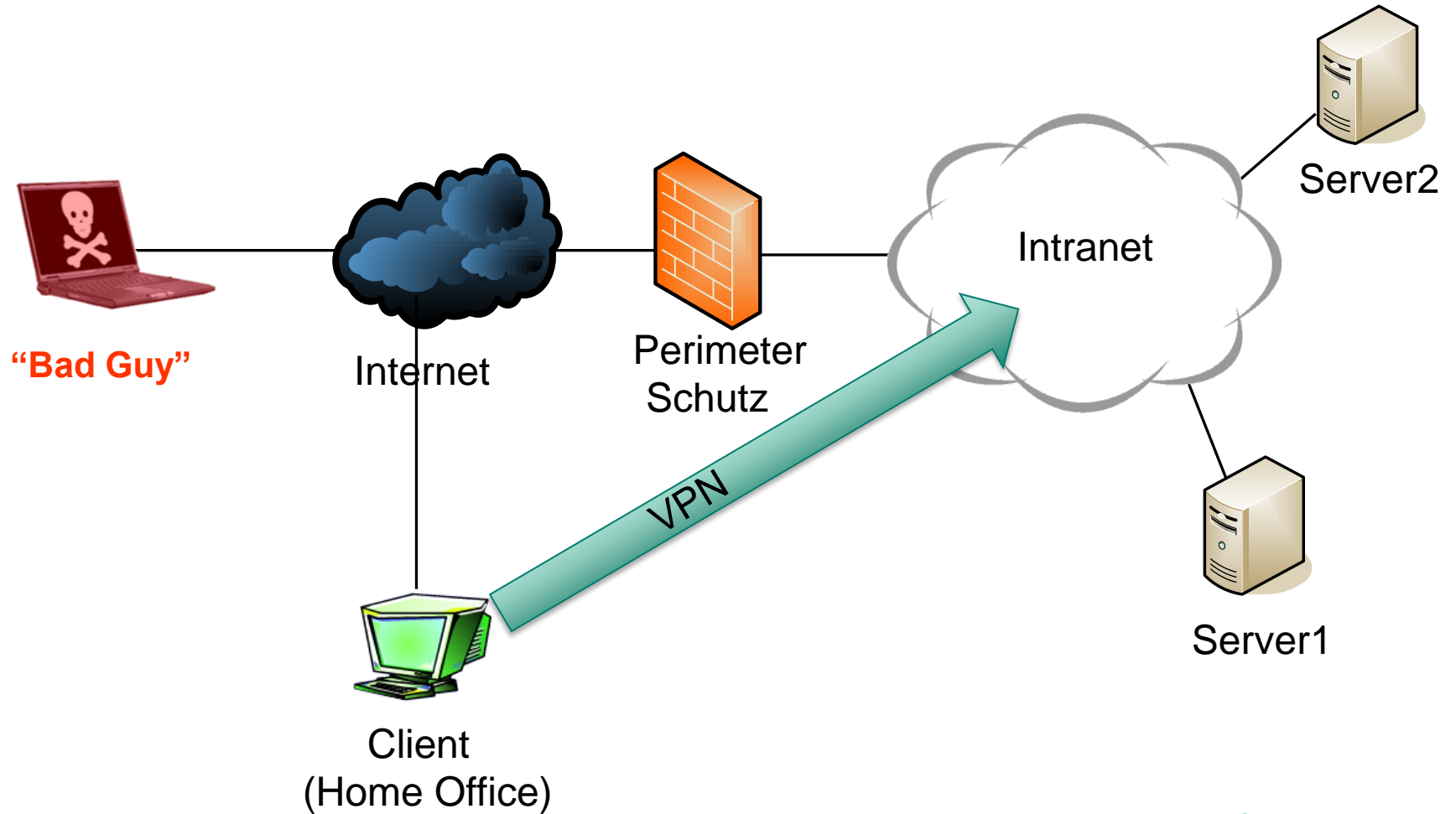
Business Development Manager S3

23.06.2009

Verlagerung der Angriffe auf den Client

- Klassisches Eindringen ins interne Netz über den Perimeter ist schwieriger geworden
- Angreifer suchen alternative Wege, um ins lokale Netz einzudringen
- Benutzer sind ein lohnendes Angriffsziel:
 - Haben Zugriff auf das interne Netzwerk
 - Teilweise sogar lokale Adminrechte
 - Sind leichter zu täuschen als Administratoren

Das Labor



Browser als Schwachpunkt

Microsoft Security Bulletin MS09-002 – Kritisch: Kumulatives Sicherheitsupdate für Internet Explorer (961260) - Mozilla Firefox

http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms09-002.mspx

Microsoft TechNet

TechNet Home | TechCenter | Downloads | TechNet Programm | Security Bulletins | Archiv | TechNet Plus Abo

Suche nach:

TechNet (DE) GO

TechNet Sicherheit

Security Bulletin-Suche

Sicherheitsempfehlungen

Produkte

Sicherheit

Tools

Events u

Newsgr

Partners

Für klein

Für den f

[TechNet Sicherheit](#) > [Security Bulletin-Suche](#)

Microsoft Security Bulletin MS09-002 – Kritisch

Kumulatives Sicherheitsupdate für Internet Explorer (961260)

Veröffentlicht: 10. Feb 2009 | Aktualisiert: 16. Feb 2009

Produkt	Schwachstelle	Betroffene Software	Schweregrad	Referenzen
Internet Explorer 7				
Windows XP Service Pack 2 und Windows XP Service Pack 3	Windows Internet Explorer 7	Remotecodeausführung	Kritisch	MS08-073 , MS08-078
Windows XP	Windows	Remotecodeausführung	Kritisch	MS08-073

administrativen Benutzerrechten arbeiten.

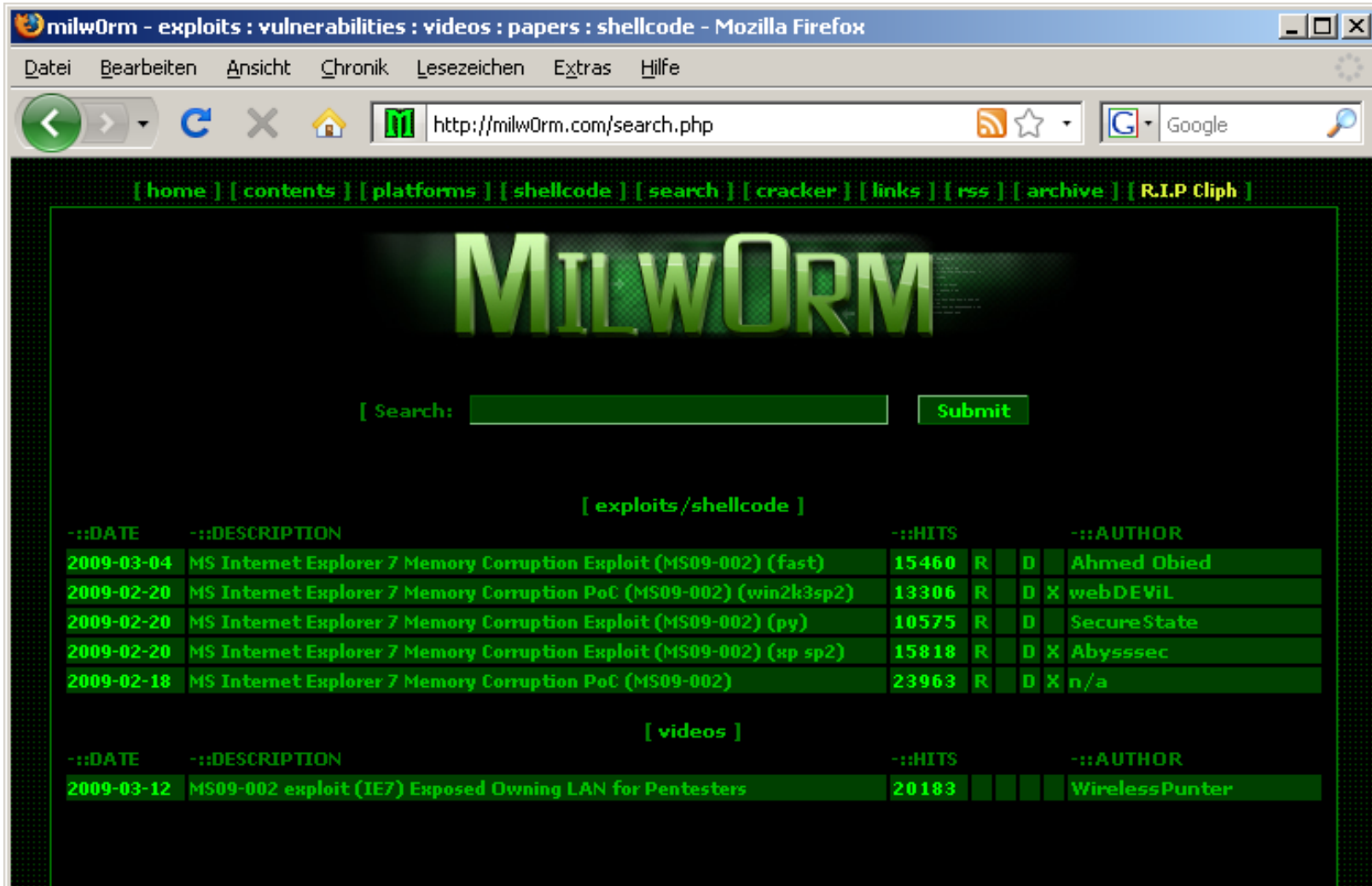
Dieses Sicherheitsupdate wird für Internet Explorer 7 unter unterstützten Editionen von Windows XP und Windows Vista als Kritisch eingestuft. Für Internet Explorer 7 unter unterstützten Editionen von Windows Server 2003 und Windows Server 2008 wird dieses Sicherheitsupdate als Mittel eingestuft. Weitere Informationen finden Sie im Unterabschnitt **Betroffene und nicht betroffene Software** in diesem Abschnitt.

Das Update behebt diese Sicherheitsanfälligkeiten, indem die Art geändert wird, wie Internet Explorer den Fehler verarbeitet, der zu der Sicherheitsanfälligkeit führt. Weitere Informationen zu den Sicherheitsanfälligkeiten finden Sie im Unterabschnitt „Häufig gestellte Fragen (FAQs)“ im nächsten Abschnitt **Informationen zu Sicherheitsanfälligkeiten**.

Fertig

Microsoft-IIS/7.0

Exploit auf der Grundlage des Patches



The screenshot shows a Mozilla Firefox browser window displaying the milw0rm website. The address bar shows the URL <http://milw0rm.com/search.php>. The website has a dark green theme with a large 'MILWORM' logo. A search bar is visible with the text '[Search:]' and a 'Submit' button. Below the search bar, there are two tables of search results. The first table is titled '[exploits/shellcode]' and lists five entries for MS09-002 exploits. The second table is titled '[videos]' and lists one entry for an MS09-002 exploit video.

[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive] [R.I.P Cliph]

MILWORM

[Search: Submit

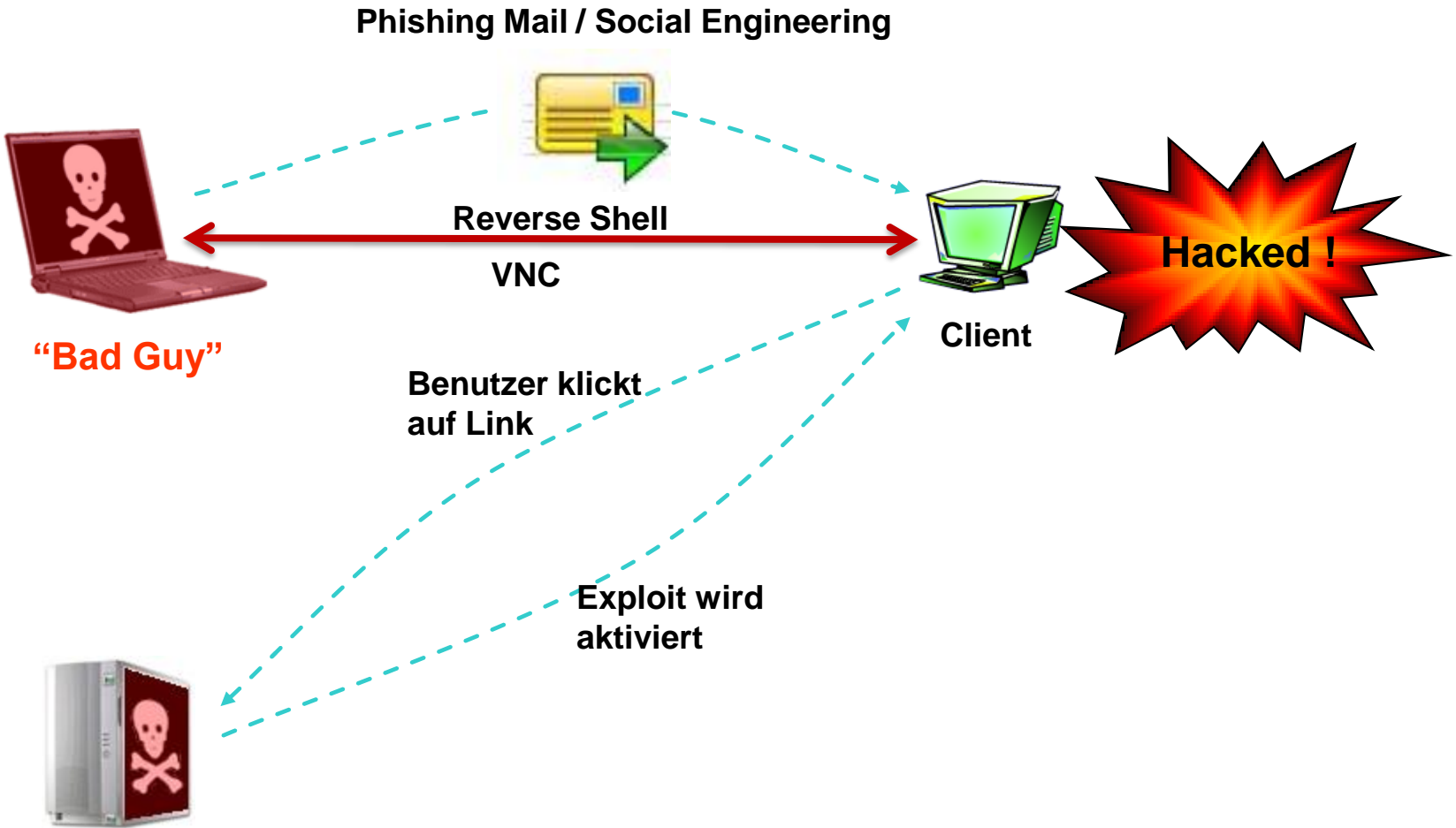
[exploits/shellcode]

--:DATE	--:DESCRIPTION	--:HITS			--:AUTHOR
2009-03-04	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (fast)	15460	R	D	Ahmed Obied
2009-02-20	MS Internet Explorer 7 Memory Corruption PoC (MS09-002) (win2k3sp2)	13306	R	D X	webDEVil
2009-02-20	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (py)	10575	R	D	SecureState
2009-02-20	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (sp sp2)	15818	R	D X	Abysssec
2009-02-18	MS Internet Explorer 7 Memory Corruption PoC (MS09-002)	23963	R	D X	n/a

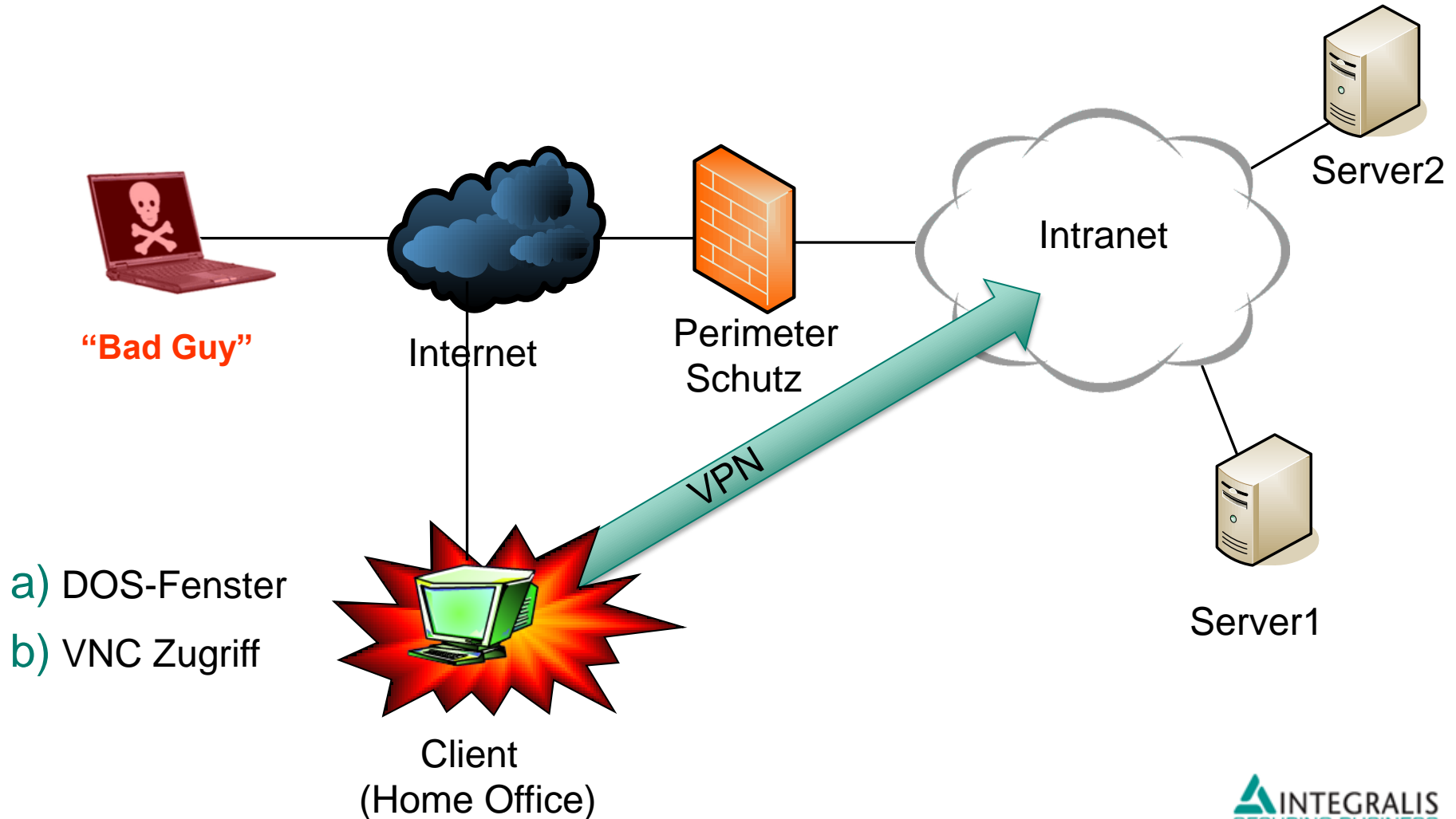
[videos]

--:DATE	--:DESCRIPTION	--:HITS			--:AUTHOR
2009-03-12	MS09-002 exploit (IE7) Exposed Owning LAN for Pentesters	20183			WirelessPunter

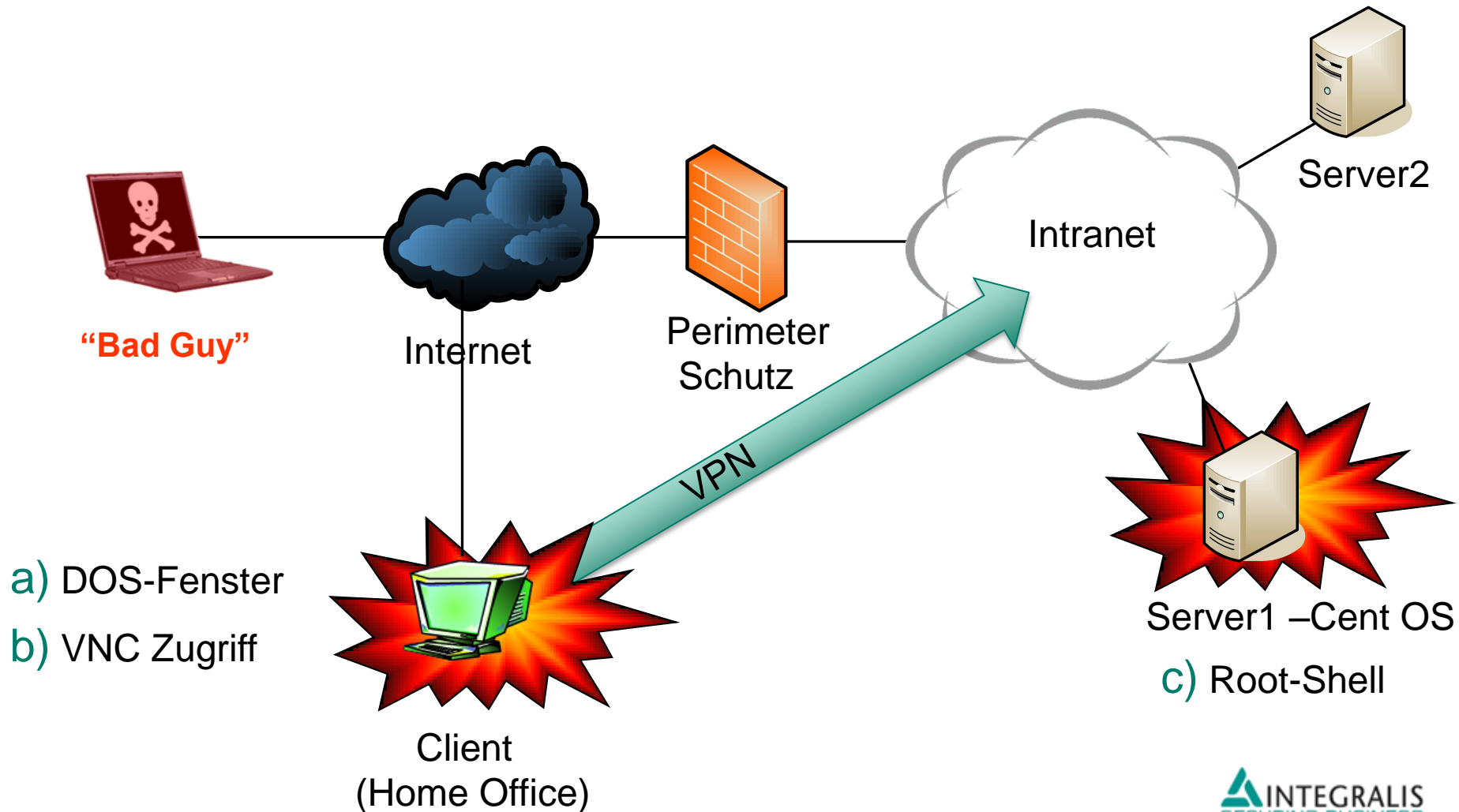
Hack #1: Übernahme des Clients



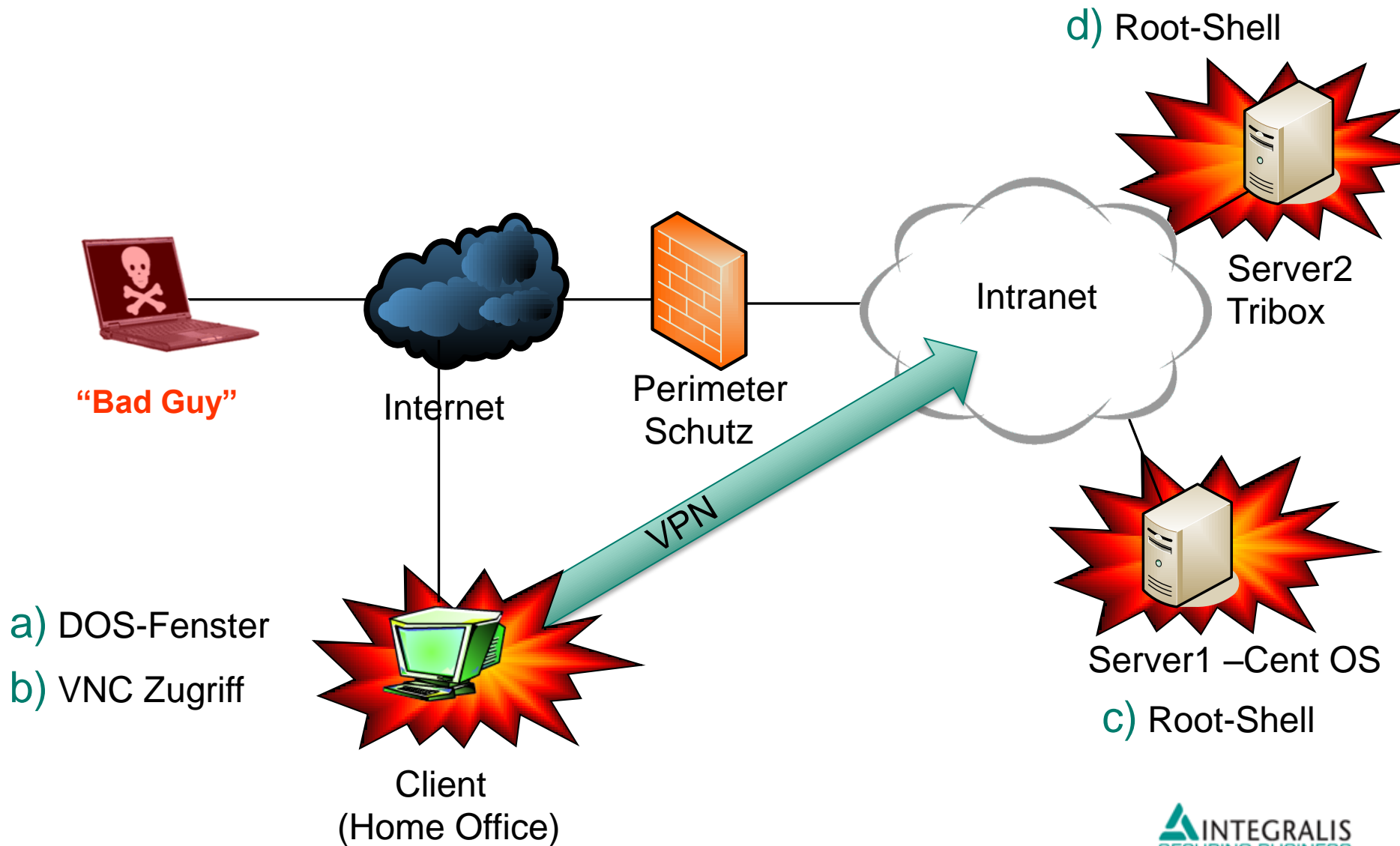
Situation nach Hack #1



Situation nach Hack #2



Situation nach Hack #3



Schutzmassnahmen

- Patchmanagement
- Absicherung der Clients
- Verhindern von ausgehenden Verbindungen
- Security Awareness (Mitarbeiter)

Fragen und Antworten



Integralis S3-Services
s3@integralis.de

Integralis[®] S3
System Security Services