

GO OUT  
IT-SECURITY  
HOSTING

BARRACUDA  
NETWORKS

SOPHOS

Symantec.

NetDefender  
IT Security Distribution

IBM

IT-Security Forum #9

Computerworld.ch

Blickpunkt ÖMT

## Live Hacking auf eine Citrix Umgebung

Ron Ott + Andreas Wisler  
Security-Consultants  
GO OUT Production GmbH  
[www.goSecurity.ch](http://www.goSecurity.ch)

GO OUT  
IT-SECURITY  
HOSTING

BARRACUDA  
NETWORKS

SOPHOS

Symantec.

NetDefender  
IT Security Distribution

IBM

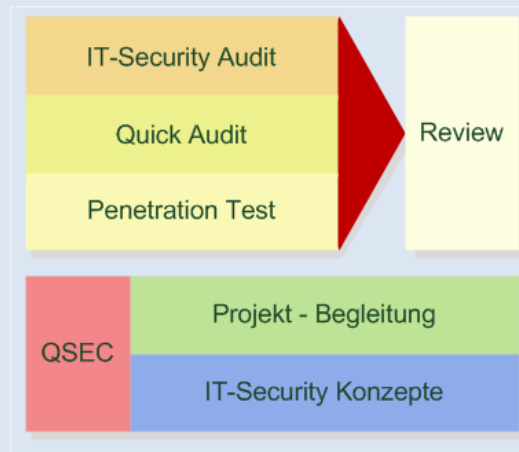
IT-Security Forum #9

Computerworld.ch

Blickpunkt ÖMT

## GO OUT Production GmbH

- Gegründet 1999
- 9 Mitarbeiter
- Dienstleistungen:



GO OUT  
IT-SECURITY  
HOSTINGBARRACUDA  
NETWORKS

SOPHOS

Symantec

NetDefender  
IT Security Distribution

IBM

IT-Security Forum #9

Computerworld.ch  
Blickpunkt: DMU

## Einleitung

- Komplette Citrix Umgebung nachgebaut
- Verschiedene Schwachstellen vorhanden
- Alles in Audits angetroffen

- Vielen Dank an Computerlinks für die Citrix Test-Lizenz

GO OUT  
IT-SECURITY  
HOSTINGBARRACUDA  
NETWORKS

SOPHOS

Symantec

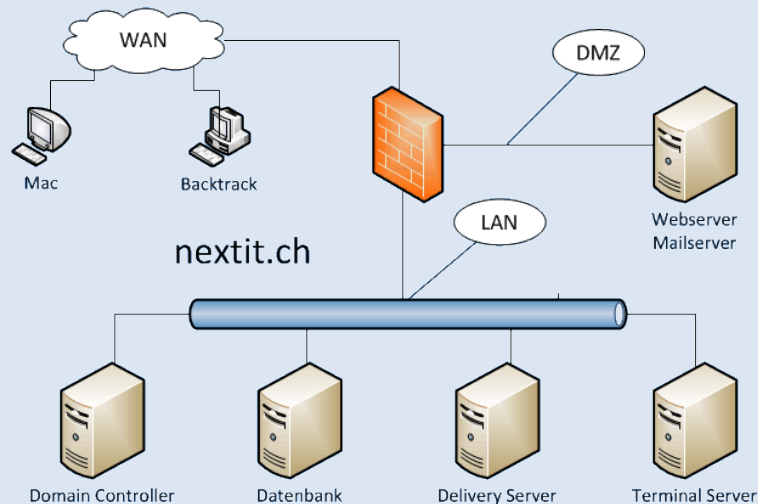
NetDefender  
IT Security Distribution

IBM

IT-Security Forum #9

Computerworld.ch  
Blickpunkt: DMU

## Netzwerk der Nextit



GO OUT  
IT-SECURITY  
HOSTING

BARRACUDA  
NETWORKS

SOPHOS

Symantec

NetDefender  
IT Security Distribution

IBM

IT-Security Forum #9

Computerworld.ch  
Blickpunkt: OMI

Site Map

Vulnerability Browser View HTTP Request / Response

Controlled Scan Retest Execute SQL Commands Get Shell Open LFI Exploitation

## Summary

Severity : Important

Confirmation : **Confirmed**

Vulnerable URL : [http://www.nextit.ch/informationen.asp?suchbegriff=""></style></script><script>alert\(0x0000D2\)</script>](http://www.nextit.ch/informationen.asp?suchbegriff=)

Vulnerability Classifications: [PCI 6.5.1](#) [OWASP A2](#) [CAPEC-19](#) [CWE-79](#) [79](#)

Parameter Name: **suchbegriff**

Parameter Type: Querystring

Attack Pattern: ""-></style></script><script>alert(0x0000D2)</script>

## Impact

There are many different attacks that can be leveraged through the use of XSS, including:

Dashboard

Scan Finished 100%

0020 / 0020

Scan Information

Current Speed : 9.3 req/sec  
Average Speed : 4.0 req/sec  
Total Requests : 317  
Failed Requests : 0  
HEAD Requests : 8  
Elapsed Time : 00:01:18

Issues (5)

Cross-site Scripting  
informationen.asp (suchbegriff)

Cookie Not Marked As HttpOnly  
/informationen.asp

ASP.NET Version Disclosure  
/

Forbidden Resource  
/includes/bilder/ [Variations:2]  
/includes/  
/bilder/

IIS Version Disclosure  
/

## Einschub : Cross-Site Scripting (XSS)

- **Javascript**: In Webseiten eingefügter Code, der im Browser ausgeführt werden
- Oft enthalten **dynamisch generierte Webseiten** die von einem Benutzer eingegebenen Daten
  - Produktresultatseiten, Google etc. zeigen den eingegebenen Suchstring an
- Bei **XSS** nutzt ein Angreifer dieses Feature aus:

GO OUT  
IT-SECURITY  
HOSTINGBARRACUDA  
NETWORKS

SOPHOS

Symantec

NetDefender  
IT Security Distribution

IBM

IT-Security Forum #9

Computerworld.ch

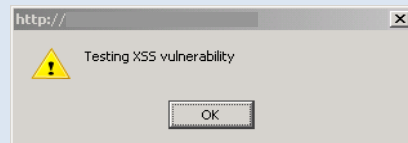
Blickpunkt: ÖMU

## Einschub : Testen auf XSS

- Eingabe eines **einfachen Javascripts** in verschiedenen Feldern von Web-Formularen:

```
<script>alert("Testing XSS vulnerability");</script>
```

- Bei Erfolg öffnet sich ein **Popup-Fenster**

GO OUT  
IT-SECURITY  
HOSTINGBARRACUDA  
NETWORKS

SOPHOS

Symantec

NetDefender  
IT Security Distribution

IBM

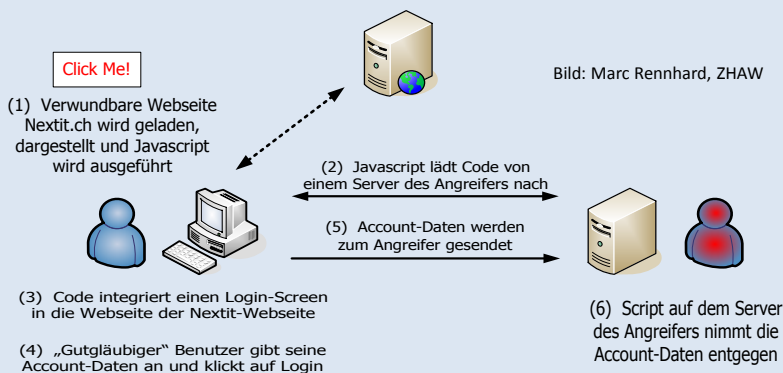
IT-Security Forum #9

Computerworld.ch

Blickpunkt: ÖMU

## Einschub : XSS-Beispiel

- Opfer hat Account für einen Web-Shop, Angreifer möchte Account-Daten erhalten.
- Angreifer hat ein entsprechendes JavaScript in einem Link in einer Nachricht in einem Web-Forum platziert, Opfer hat die Nachricht geöffnet.



GO OUT  
IT-SECURITY  
HOSTINGBARRACUDA  
NETWORKS

SOPHOS

Symantec

NetDefender  
IT Security Distribution

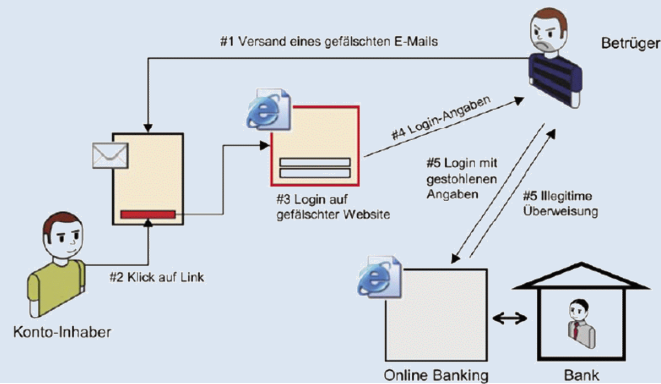
IBM

IT-Security Forum #9

Computerworld.ch  
Blickpunkt: OMI

## 2. Ausnutzen der gefundenen Schwachstellen

- Mailversand Intern → Intern ohne Authentifizierung
  - Mail hat hohe Glaubwürdigkeit, da vom korrekten Server
- Phishing-Angriff auf Mitarbeiterin Karin Lanz
  - Variante mit XSS der Webseite
  - Variante Nachbau Loginseite mit ähnlichem Namen «NEXTTIT.CH»

GO OUT  
IT-SECURITY  
HOSTINGBARRACUDA  
NETWORKS

SOPHOS

Symantec

NetDefender  
IT Security Distribution

IBM

IT-Security Forum #9

Computerworld.ch  
Blickpunkt: OMI

## 3. Citrix Login

- Kann Applikation «verlassen» werden?
- Lassen sich interessante Programme / Daten finden?
- Kann CMD ausgeführt werden?
- Können Daten auf den Terminal Server kopiert werden?
- Können Programme installiert werden?
- Kann das Antivirenprogramm «überlistet» werden?
- Kann Schadcode ausgeführt werden?
- Sind Passwörter ersichtlich?
- Ist der Administrator angreifbar?
- Kann der Server «übernommen» werden?



GO OUT  
IT-SECURITY  
HOSTINGBARRACUDA  
NETWORKS

SOPHOS

Symantec.

NetDefender  
IT Security Distribution

IBM

IT-Security Forum #9

Computerworld.ch

Blickpunkt: KMU

### 3. Citrix Login

- Uptime

IP	Uptime	User Accounts	Sen
195d 18h 27m 25s		S	htg...
194d 16h 39m 21s		A	Ga...
194d 13h 26m 2s		A	co...
192d 21h 43m 50s		G	LM
169d 6h 34m 1s		S	htg...
163d 1h 27m 4s		A	m...
155d 6h 52m 57s		G	LM
134d 18h 46m 17s		G	LM
125d 22h 16m 9s		G	LM
125d 33m 59s		A	A...
119d 14h 29m 43s		A	Ga...
44d 23h 45m 8s		A	not...
26d 11h 26m 52s		A	r...
26d 11h 20m 37s		A	r...
16d 13h 47m 48s		A	pn...
6h 38m 39s		A	LM
6h 38m 18s		A	pn...

GO OUT  
IT-SECURITY  
HOSTINGBARRACUDA  
NETWORKS

SOPHOS

Symantec.

NetDefender  
IT Security Distribution

IBM

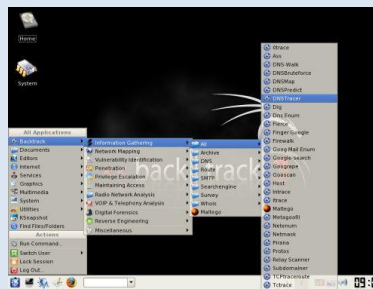
IT-Security Forum #9

Computerworld.ch

Blickpunkt: KMU

### Einschub Backtrack / Metasploit

- Backtrack
  - BackTrack basiert auf Ubuntu und bietet zahlreiche Tools für Penetrationstests, mit denen Anwender und Administratoren die Sicherheit von Systemen testen können. Dazu gehören Sniffer für LAN und WLAN, Passwort-Cracker und Schwachstellenscanner.
- Metasploit
  - Metasploit unterstützt Penetrationstests, Entwicklung von IDS-Signaturen sowie die Exploit-Forschung. Es enthält über 450 Exploits und zahlreiche Payloads, also den eigentlichen Code, um irgendeine Funktion auf dem kompromittierten System auszuführen.



GO OUT  
IT-SECURITY  
HOSTINGBARRACUDA  
NETWORKS

SOPHOS

Symantec.

NetDefender  
IT Security Distribution

IBM

IT-Security Forum #9

Computerworld.ch

Blickpunkt: OMI

## 4. Vorgehen

- Alternative DOS-Shell ausführen [Virustotal](#)
- Payload «erstellen», welche vom AV nicht erkannt wird
- Zugriff von innen nach aussen aufbauen
  - Mit Metasploit weiterfahren
- Suche nach spannenden Informationen
  - Skripts
  - Zus. Server (Test-Server)
  - Freigaben
  - Backup-Dateien
  - Passwort-Dateien
  - ...

GO OUT  
IT-SECURITY  
HOSTINGBARRACUDA  
NETWORKS

SOPHOS

Symantec.

NetDefender  
IT Security Distribution

IBM

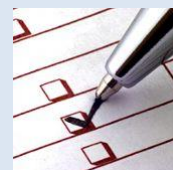
IT-Security Forum #9

Computerworld.ch

Blickpunkt: OMI

## Fazit

- Ausgenutzte Schwachstellen:
  - XSS auf Homepage
  - Interner Mailversand
  - Phishing / Social Engineering
  - Ungenügend gehärtete Citrix-Umgebung
  - Test-Server nicht geschützt
  - Freigaben / NTFS-Rechte nicht genügend eingeschränkt
  - Wichtige Informationen in Skripts bzw. Skript änderbar



GO OUT  
IT SECURITY  
HOSTING

BARRACUDA  
NETWORKS

SOPHOS

Symantec

NetDefender  
IT Security Distributor

IBM

IT-Security Forum #9

Computerworld.ch

Blickpunkt ÖML

## Zusammenfassung

### Wichtig für die Geschäftsleitung

- IT-Sicherheitskonzept erstellen
- Kontrolle der Konfiguration veranlassen
  - Besonders wichtig bei von Extern erreichbaren Systemen

### Wichtig für die IT

- Restriktive Konfiguration vornehmen
- Test-Systeme in Wartung aufnehmen (AV, Patchen, Firewall, etc.)
- Nie sensitive Informationen in Klartext speichern

### Wichtig für Benutzer

- Sensibilisierung
- GMV (Gesunder MenschenVerstand)