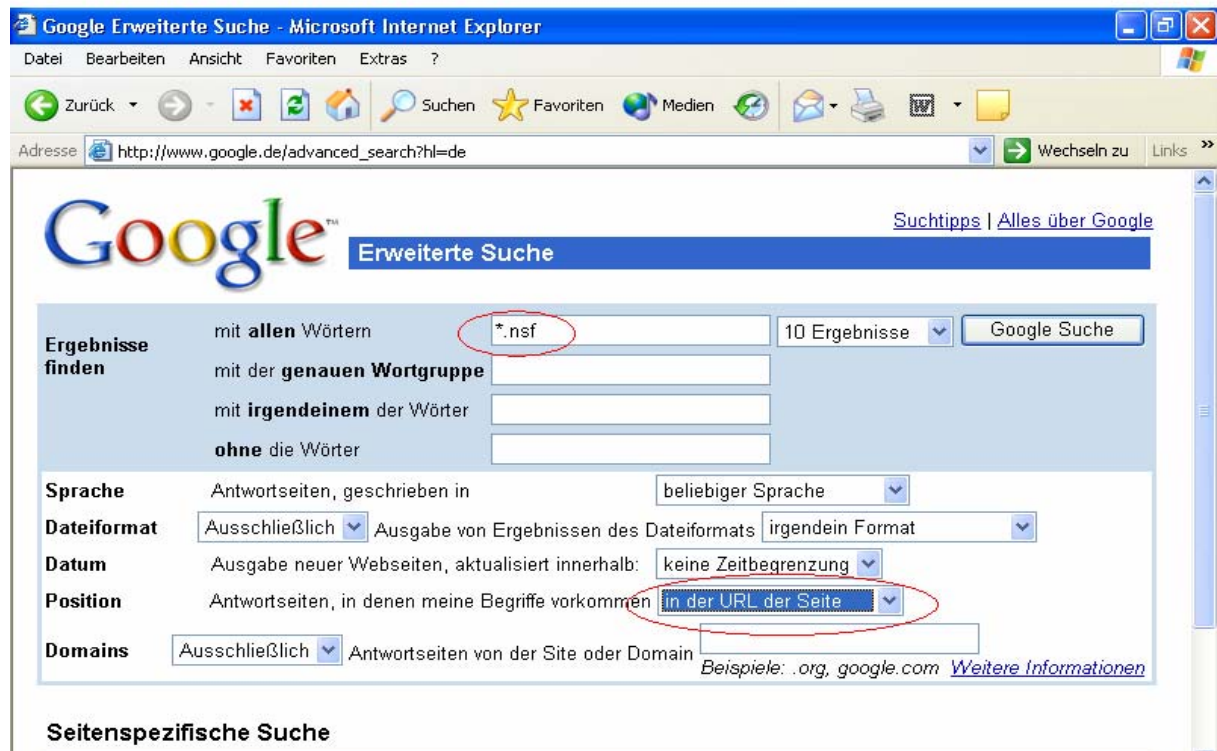


„Hackerziel“ Domino

IBM Lotus Domino gilt als sehr sichere Plattform für interaktive Webanwendungen. Wie sieht es mit der Wirklichkeit aus? Um es vorwegzunehmen, kommt es auf die Konfiguration an. Unsichere Konfigurationen bieten für Hacker ein leichtes Entrance in eine Domino Infrastruktur. Unternehmenskritische Daten werden unbemerkt entwendet oder zerstört. Es stellt sich die Frage: „Ist es möglich Domino aus dem Web zu hacken? Und wenn ja, wie und was kann man dagegen tun?“

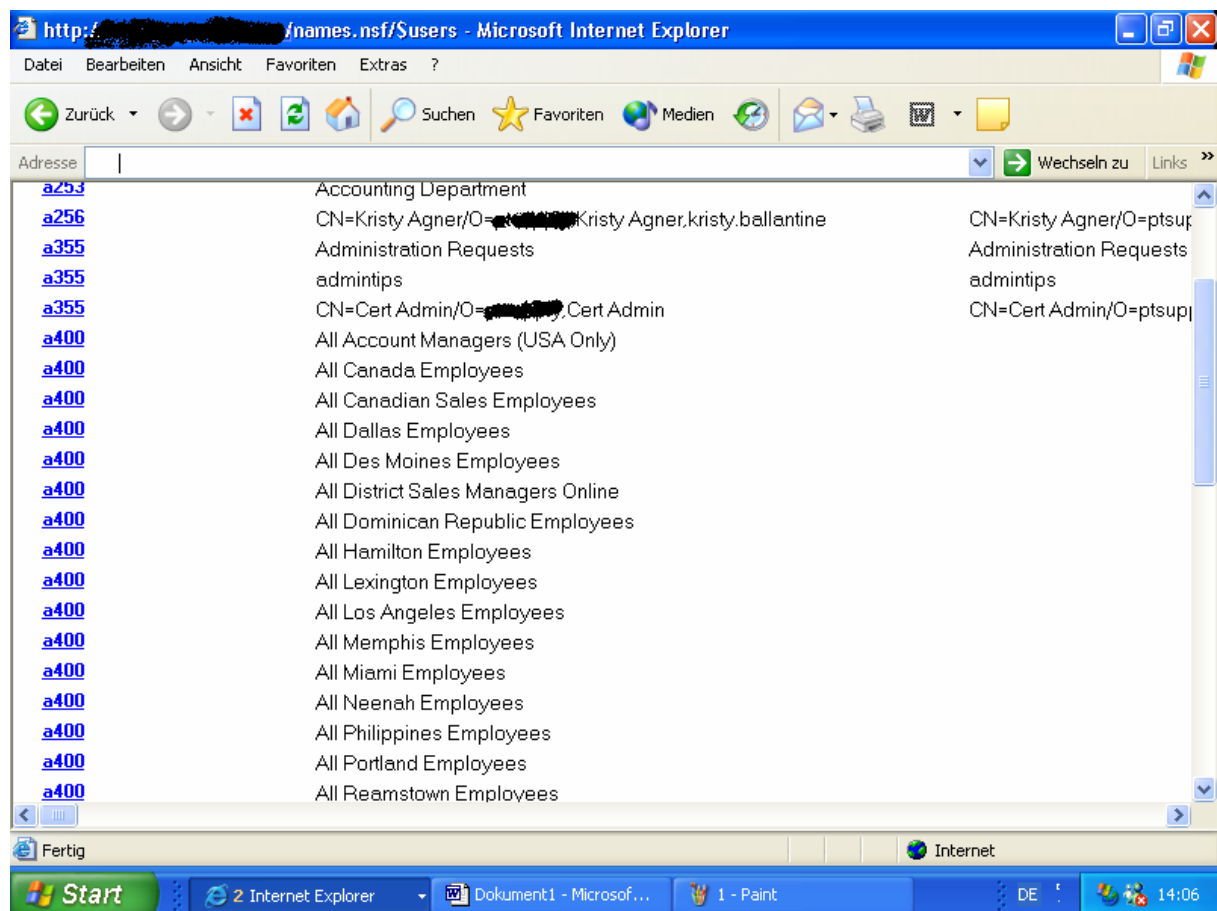
Zur Erläuterung beginnen wir an der Wurzel. Da wäre zunächst das fingerprinting. Mit Hilfe von fingerprinting suchen die „Hacker“ ihre Opfer. Bei Domino ist das relativ einfach: Wir brauchen eine nette Datenbankerweiterung mit Namen *.nsf, einen Browser, der Internetsdienst Google und los geht es:



So einfach kann man Google als Hackerhilfe nutzen. Durch Suche der *.nsf bekommt man eine Liste mit tausenden von Opfern. Dem Hacker kommt es dabei auf Schwachstellen in der Konfiguration an. Diese gilt es aufzudecken. Die Zauberformel heißt hier: „Standardkonfiguration“. Im Web gibt es tausende Dominoserver, welche „Default“ konfiguriert sind und lassen somit den Gedanken an weit geöffnete Scheunentore freien lauf.

Nun geht es richtig los. Aus Datenschutzgründen wurden Informationen des Opfers unkenntlich gemacht.

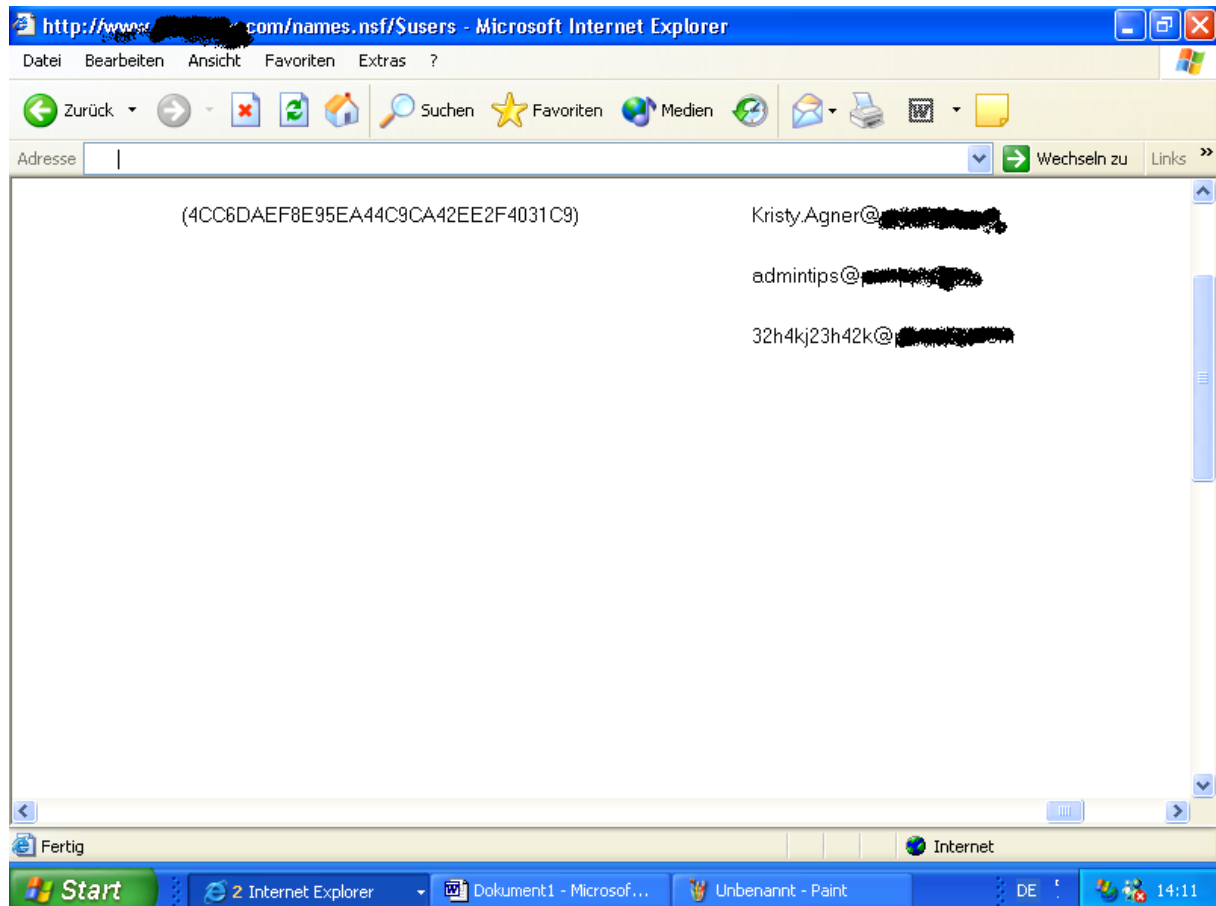
Zunächst geht die Suche weiter nach offenen Domino Verzeichnissen. „Bingo“: Hunderte von offenen Domino Verzeichnissen sind frei zugänglich, und wenn man drin ist, sieht das so aus:



Hier wurde die URL **http://opfer.com/names.nsf/\$users?Openview** verwendet um nicht die Java Applet Ansicht „People“ zu erhalten.

Das schöne für den Hacker in dieser Ansicht ist, dass die Internetpasswort - Hashes hier angezeigt werden. Man muss in dieser Ansicht sehr weit nach rechts scrollen. Ein „Doppel-Bingo“: Internetpasswort-Hashes. Hier der Hash für den Benutzer Kristy Agner: 4CC6DAEF8E95EA44C9CA42EE2F4031C9.

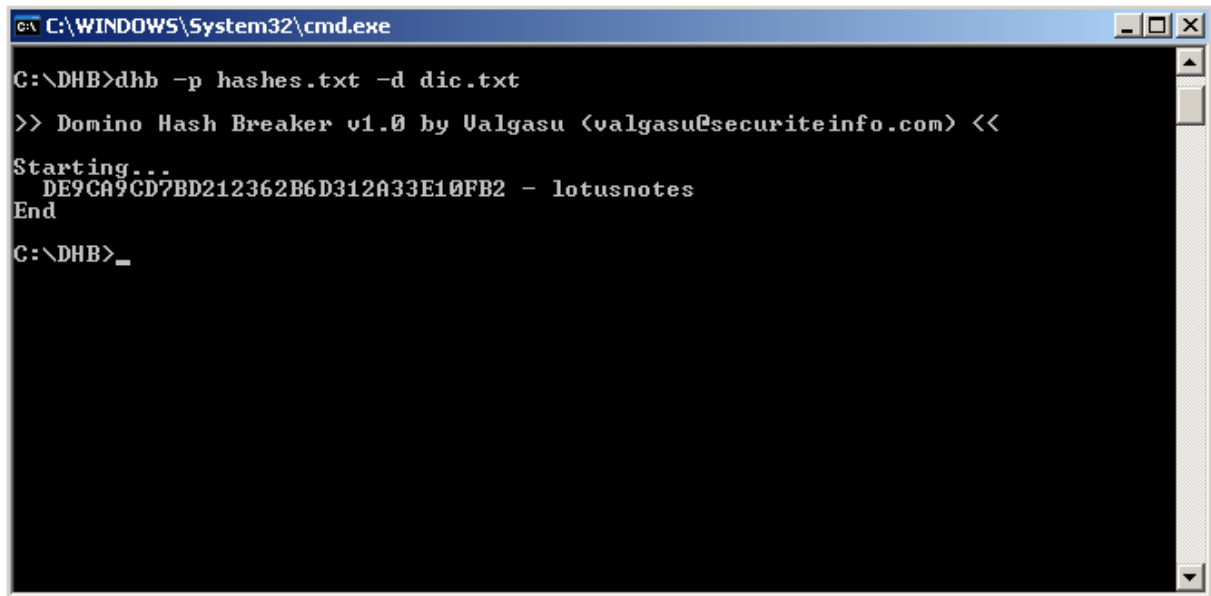
Dabei bietet Domino ab der Version 5 sogenannte „salted hashes,“ gesalzene Verschlüsselung an. Diese kann mit der Option „Sichere Internet Passwörter verwenden“ im Domino-Administrator eingestellt werden.



Im nächsten Step wird es richtig gefährlich. Die Internetpasswörter sind zwar verschlüsselt aber, wie der Fachmann sagt: „unsalted“ (ungesalzen) verschlüsselt. Das bedeutet, dass die Verschlüsselung jeder Zeichenfolge immer das gleiche Ergebnis liefert. So liefert das überaus beliebte Passwort:

„lotusnotes“ immer den folgenden hash (DE9CA9CD7BD212362B6D312A33E10FB2)

Es gibt Tools, die den Hash sofort entschlüsseln, entweder mit einem „Directory“- Attack, der einfach eine Wörterliste verwendet oder einer „Bruteforce“-Attack, die durch systematisches probieren zum Ziel kommt.



```
C:\WINDOWS\System32\cmd.exe
C:\DHB>dhb -p hashes.txt -d dic.txt
>> Domino Hash Breaker v1.0 by Valgasu (valgasu@securiteinfo.com) <<
Starting...
DE9CA9CD7BD212362B6D312A33E10FB2 - lotusnotes
End
C:\DHB>_
```

Es erübrigt sich zu erwähnen dass meistens das Internetpasswort auch das USER.ID Passwort ist. Und außerdem, die meisten Administratoren bei der Registrierung neuer Benutzer auch noch die User.ID im Dominoverzeichnis abspeichern. Man braucht dann nur noch auf die ID-Datei im Personendokument zu klicken, Sie herunterladen, und schon hat man eine gültige USER.ID. Sollte das Internetpasswort **nicht** mit dem USER.ID Passwort übereinstimmen, gibt es auch hierfür Tools, die das Kennwort genauso herausbekommen, wie es auch DHB.EXE macht.

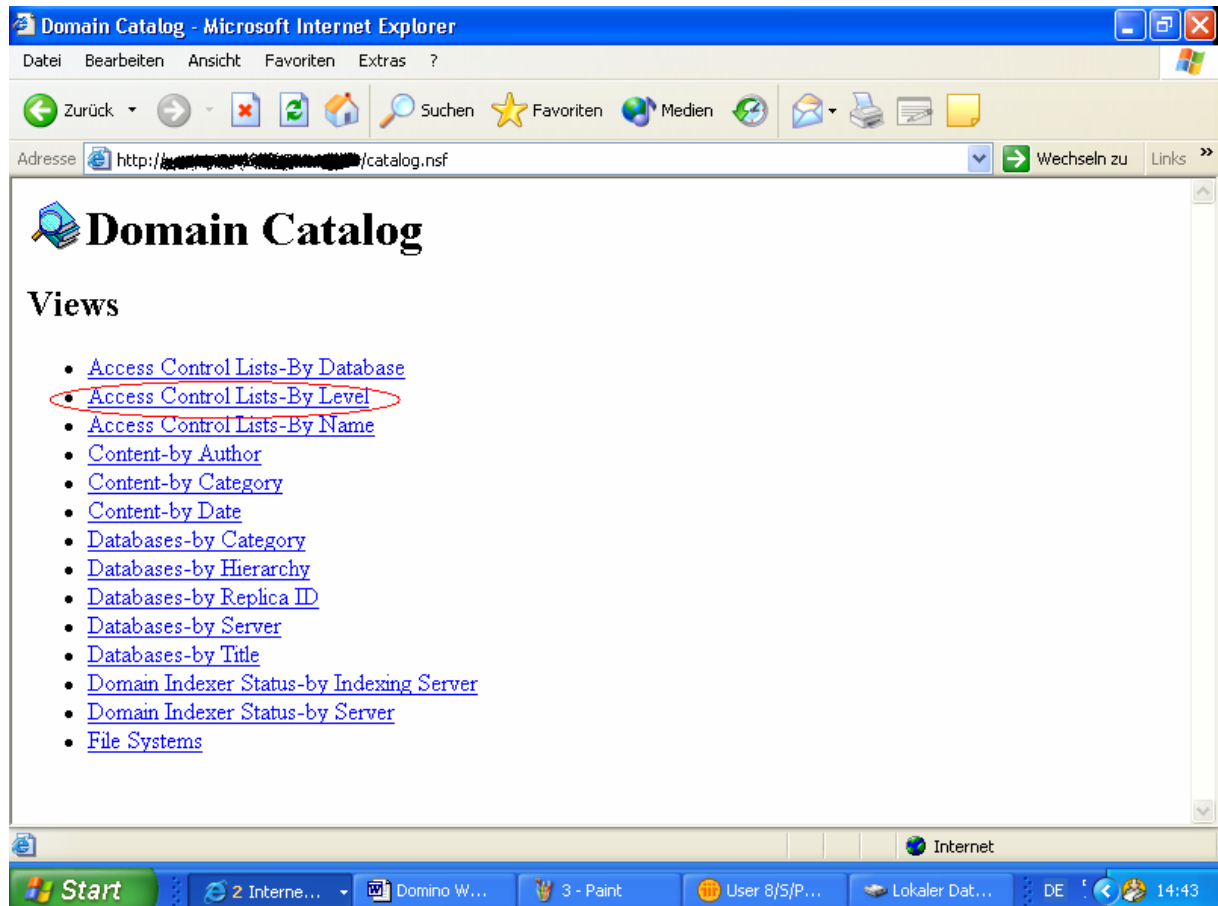
Je nach Domino Version ist in der NAMES.NSF standardmäßig der Anonymous auf „Reader“ gesetzt. Erst die neueren Versionen setzen den Benutzer Anonymous auf „Keinen Zugriff“. Jeder Webbrowser versucht Web-Seiten als Benutzer Anonymous zu öffnen, nur wenn der Zugriff verweigert wird, erhält man ein Login Fenster. Im Falle von Domino haben ältere Versionen gar keinen Eintrag in der ACL für den Benutzer Anonymous, oder er ist auf Reader in der ACL eingestellt.

„Kalter Kaffee“?: „Es ist klar dass man die ACL einstellt wenn man einen Server ins Internet stellt.“

So klar ist das nicht, es gibt dutzende Server von großen Unternehmen, wo der Zugriff möglich war. Häufig werden in diesen Unternehmen Anwendungen geschrieben die auf das Domino Verzeichnis zugreifen, und dann wird, nur zum Testen der Anwendung durch den Programmierer, die ACL geändert. Später wird dann vergessen, dass die ACL zurückgestellt werden muss. Oft fehlt es neuen Administratoren an Wissen die ACL richtig zu verwalten. Es gibt auch Server die bereits gehackt und ein sogenannter „Bots“ (Robots) sind → Das sind „Sklaven“ für den Hacker, mit denen er alles machen kann. Checken Sie die ACL aller Datenbanken auf Ihren Webservern regelmäßig um solche Angriffe zu vermeiden.

Es gibt aber auch andere Systemdatenbanken die von Haus aus bei Domino frei zugänglich sind, natürlich abhängig von der verwendeten Version. Besonders gefährlich ist die Catalog.nsf.

Nächster Versuch:



Auch hier werden wir über Google.com fündig. Gleiches Spiel. Jetzt sucht man nur noch in der Ansicht „Access Control by Level“ die Opfer Datenbanken aus. Fertig!!!

Diese Beispiele sind wirklich live aus dem Internet, und wie schon erwähnt, die Namen haben wir aus verständlichen Gründen geschwärzt.

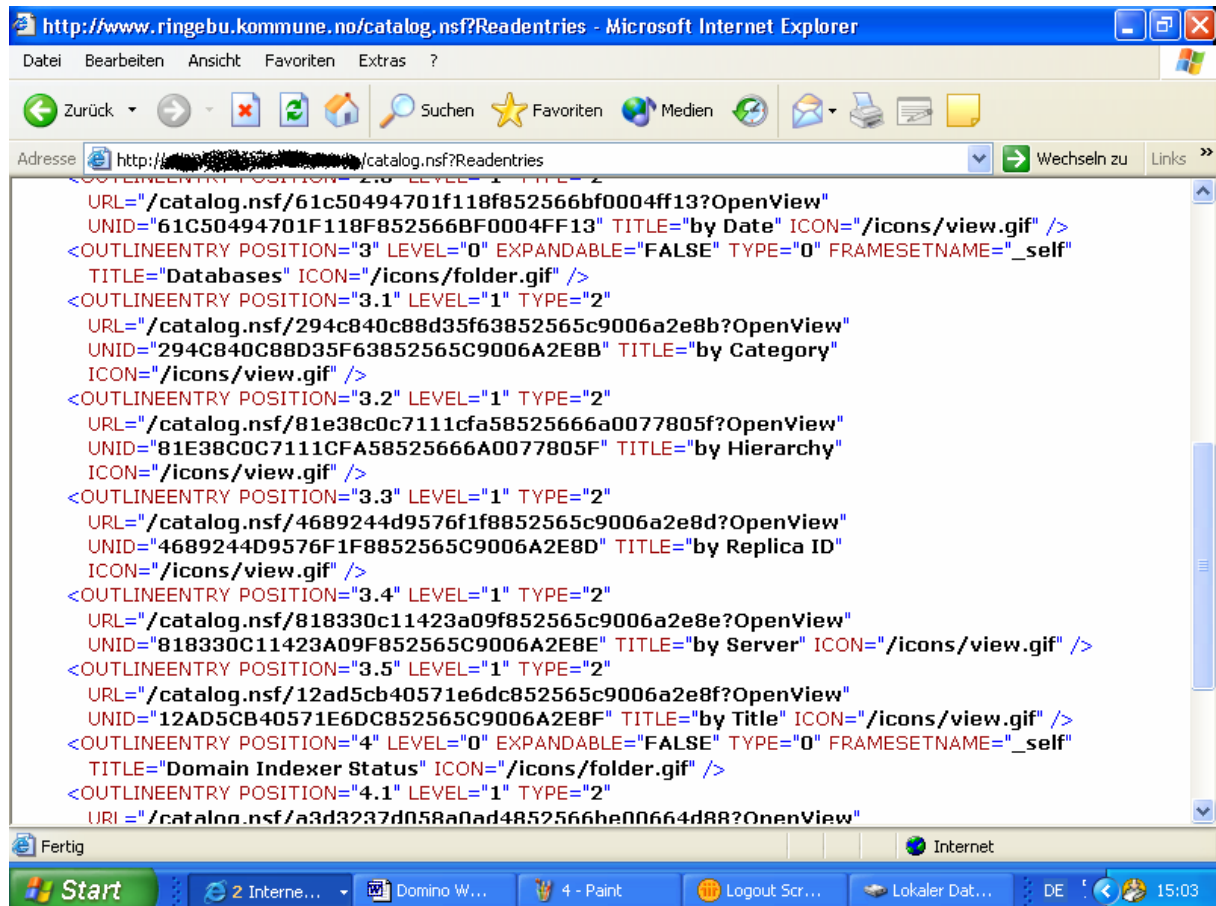
Überprüfen Sie peinlichst die ACLs Ihrer Server und Datenbanken, um Hackern keine Chance zu geben.

Noch ein weiteres Problem:

Viele Domino Entwickler verursachen Sicherheitsprobleme innerhalb der Domino Infrastruktur eines Unternehmens. Zunächst geben sie in Webanwendungen in der ACL für den Benutzer Anonymous Autor Zugriff ein, weil sie oft Masken zum Anfragen von Informationen bereitstellen. Viel besser wäre es doch die Masken für den öffentlichen Zugriff (Public Access) freizugeben, dann kann man dem Benutzer Anonymous in der ACL auch „No Access“ geben. Er kann trotzdem im Internet z.B. Anmeldemasken ausfüllen. Websites sollten immer mit PublicAccess-Masken arbeiten, denn wenn man dem Anonymous das Recht „Reader“ gibt, dann hat er Lesezugriff auf alle Dokumente in der Datenbank.

Ein anderes Problem sind die Features von Domino die man nicht ohne weiteres abstellt. So zum Beispiel das XML Feature. Mit ein bisschen Wissen ist es einfach eine Liste aller Ansichten einer Datenbank zu erhalten, auch wenn der Designer das nicht so unbedingt geplant hatte.

Hier ein nettes URL Kommando: <http://opfer.com/homepage.nsf?ReadEntries>



Hier erhält man eine Liste aller Ansichten einer Datenbank, sogar mit dazugehöriger URL. Wunderbar! Diese URL wird kopiert und in einen Browser eingefügt. Jetzt erhält man Ansichten die normalerweise nicht zu sehen sein sollten. Was kann man dagegen tun? Es empfiehlt sich die Ansicht zu verstecken, oder besser, in den Gestaltungseigenschaften der Ansicht die Option „Verbergen in Webbrowsern“ zu aktivieren, damit sie wirklich nicht im Web zu sehen ist.

Sie sehen also, vieles ist möglich, erschreckend mehr als wir hier beschreiben können. Die einzige Möglichkeit des Schutzes ist, niemals Standardeinstellungen zu übernehmen und die Entwickler und Administratoren schulen, schulen, schulen, damit Sie relativ sicher vor Webangriffen sind. Fördern Sie aktiv das Sicherheitsbewusstsein in Ihren Unternehmen.

Das Training zu diesem Thema wird in Deutschland exklusiv über das Unternehmen Com-Education and Consulting GmbH angeboten. <http://www.com-education.de>