VIRTUALAB

SIMULATION EINER IT-SICHERHEITSUMGEBUNG BESCHREIBUNG UND ANLEITUNG

Christoph Bucher

christoph.bucher@hslu.ch

Version: 1.0

Datum: 14.01.2011

Inhaltsverzeichnis

1 Einleitung

1.1 Zweck des vorliegenden Dokuments

Dieses Dokument soll eine kurze Übersicht über die Simulationsumgebung **„VirtuaLAB“** verschaffen, welche im Zusammenhang des Leitprogramms „**Gefahren aus dem Internet: Ein interaktives Leitprogramm für die Sekundarstufen I/II“** entwickelt wurde. Die Simulationsumgebung und das Leitprogramm sollen es den Studierenden ermöglichen, die Gefahren, welche im Internet lauern, auf eine interaktive Art erfahrbar zu machen und ihnen Wege aufzeigen, wie sie diese erkennen und sich vor ihnen schützen können.

Das Leitprogramm ist unter folgender URL vorzufinden:
http://www.swisseduc.ch/informatik/internet/gefahren_aus_dem_internet

Die Simulationsumgebung ist unter folgender URL vorzufinden:
http://www.virtualab.ch

1.2 Aufbau des vorliegenden Dokuments

Dieses Dokument gliedert sich in zwei Hauptteile. Der erste Teil dient einer allgemeinen Beschreibung der Simulation und illustriert die notwendigen Schritte, um die Simulation im Klassenzimmer betreiben und administrieren zu können und gibt einen Überblick über die wichtigsten Funktionen. Im zweiten Teil werden die Systemanforderungen und weitere technische Informationen zur Simulation aufgeführt. Es handelt sich dabei nicht um ein Systemhandbuch, welches sämtliche programmiertechnsiche Aspekte bis ins Details auslotet.

2 Beschreibung der Simulation

2.1 Allgemeines

Bei der Simulationsumgebung („VirtuaLAB“) handelt es sich um eine webbasierte Anwendung. Damit sie genutzt werden kann, ist eine aktive Internetverbindung unumgänglich.

Grundsätzlich besteht die Anwendung aus zwei Komponenten:

- Das Administrationsinterface, mit Hilfe dessen die Lehrperson eigene Klassen anlegen sowie in die Simulation eingeloggte Studierende administrieren kann
- Die eigentliche Simulationsoberfläche, mit welcher die Studierenden arbeiten. Hierbei stehen die zwei Anwendungsbereiche „E-Mail“ sowie „WWW“ zur Auswahl. Letzterer besteht seinerseits aus zwei separaten Simulationsoberflächen (Desktopoberfläche des Opfers und Angreiferinterface)

Grundlegende Kenntnisse in der Bedienung eines Computers (E-Mail-Programm, Browser, …) genügen, um die Simulation verwenden zu können. Dies gilt für Studierende wie auch für Lehrpersonen.

2.2 Die Startseite der Simulation

Abbildung 2-1 zeigt die Einstiegsseite ins VirtuaLAB, wie sie unter der URL *http://www.virtualab.ch* abrufbar ist. Gelb markiert sind die Links, welche zur Administrationsoberfläche, bzw. zu den einzelnen Simulationsoberflächen führen.

- Link 1 startet die Simulation „E-Mail“. Details zu dieser Simulation stehen in 0
- Die Links unter 2 starten die Simulation „WWW“. Der obere Link öffnet die Desktopoberfläche des Opfers, der untere Link das Angreiferinterface. Weitere Details hierzu stehen in 2.6
- Link 3 führ zum Login des Administrationsinterfaces. Details hierzu stehen in 2.3

Abbildung 2-1: Startseite von www.virtualab.ch

2.3 Administration der Simulation

2.3.1 Registrierung und Login

Bevor Studierende sich unter einem bestimmten Klassennamen in die Simulation einloggen können, muss diese Klasse von einer Lehrperson über das Administrationsinterface angelegt werden. Damit die Lehrperson Zugang zum Administrationsinterface erhält, ist eine einmalige, kostenlose Registrierung auf der VirtuaLAB Webseite notwendig.

Login und Passwort-Reset

Abbildung 2-2 zeigt das Login-Formular des Administrationsinterfaces. Lehrpersonen können sich hier mit ihren gültigen Login-Informationen anmelden. Falls das Passwort vergessen gegangen ist, erreicht man über den Link 2 ein Formular, welches die Eingabe einer E-Mail-Adresse verlangt. Ein neues Passwort wird daraufhin an diese Adresse versandt.

Registrierung

Wer noch nicht im Besitz eines Logins ist, kann sich durch Klicken des in Abbildung 2-2 markierten Links 1 registrieren. Die Registrierung erfolgt in wenigen Schritten durch Eingabe entsprechender Daten (Name, Benutzername, E-Mail, Schule, Passwort). Wichtig ist, dass eine gültige E-Mail-Adresse angegeben wird, auf welche die Lehrperson auch Zugriff hat. Im Falle eines vergessenen Passwortes wird

das neue Passwort nämlich an die E-Mail-Adresse versandt, welche während des Registrierungsprozesses angegeben wird.

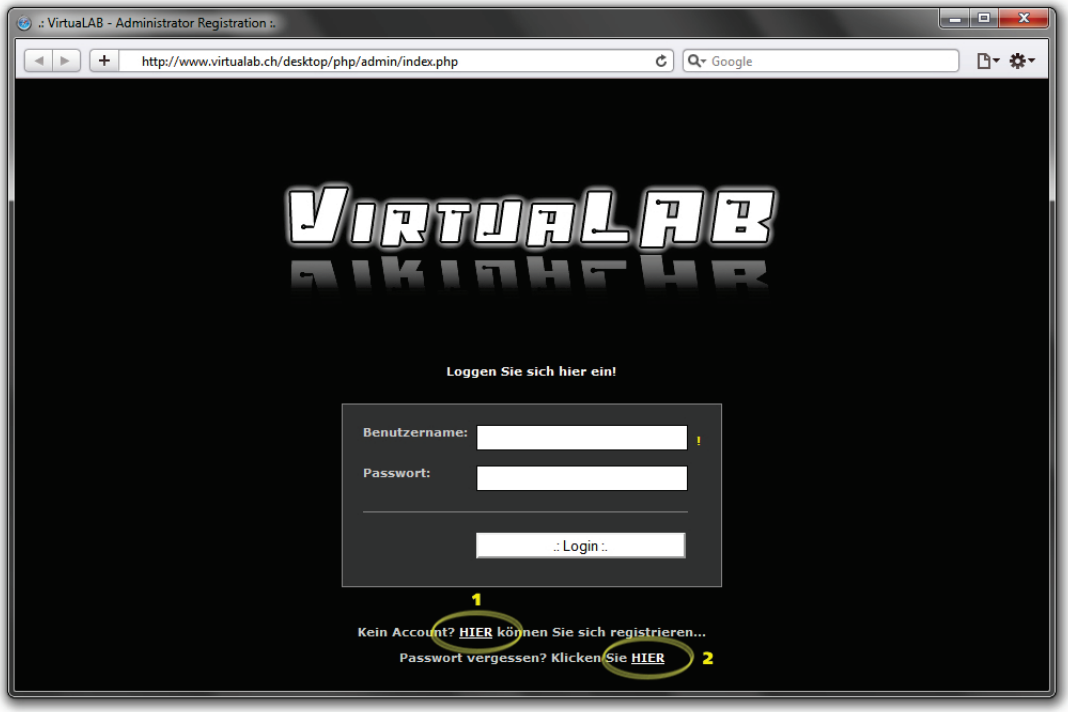

Abbildung 2-2: Registrierung und Login

2.3.2 Administrieren von Klassen und Benutzern (Studierende)

Abbildung 2-3 zeigt das Administrationsinterface nach erfolgreichem Login. Es bietet der Lehrperson zum einen die Möglichkeit, das eigene Passwort für den Administrationsbereich zu ändern, zum andern können Klassen angelegt oder gelöscht, sowie die Accounts der Studierenden verwaltet werden.

Anlegen und löschen von Klassen

Um eine neue Klasse zu erstellen, ist ein entsprechender Klassenname in das unter 1 markierte Feld einzugeben und die Schaltfläche *Erstellen* zu klicken. Ein Klassennamen darf nur einmal im System vorkommen – wird versucht eine Klasse mit gleichem Namen anzulegen, erscheint eine entsprechende Warnmeldung. Es gilt zu beachten, dass Leerzeichen im gewählten Klassennamen automatisch mit Unterstrichen ersetzt werden. Ebenso werden alle Grossbuchstaben in Kleinbuchstaben gewandelt.

In der unter 2 markierten DropDown-Box erscheinen alle Klassen, welche die momentan im Administrationsinterface eingeloggte Lehrperson angelegt hat. Um eine bestimmte Klasse zu löschen, muss Sie mit der DropDown-Box ausgewählt und die Checkbox rechtes davon selektiert werden. Durch anschliessendes Klicken auf den Link *löschen* wird die Klasse daraufhin unwiderruflich aus dem System entfernt. Alle unter diesem Klassennamen am System angemeldeten Benutzer werden ebenfalls aus dem System gelöscht.

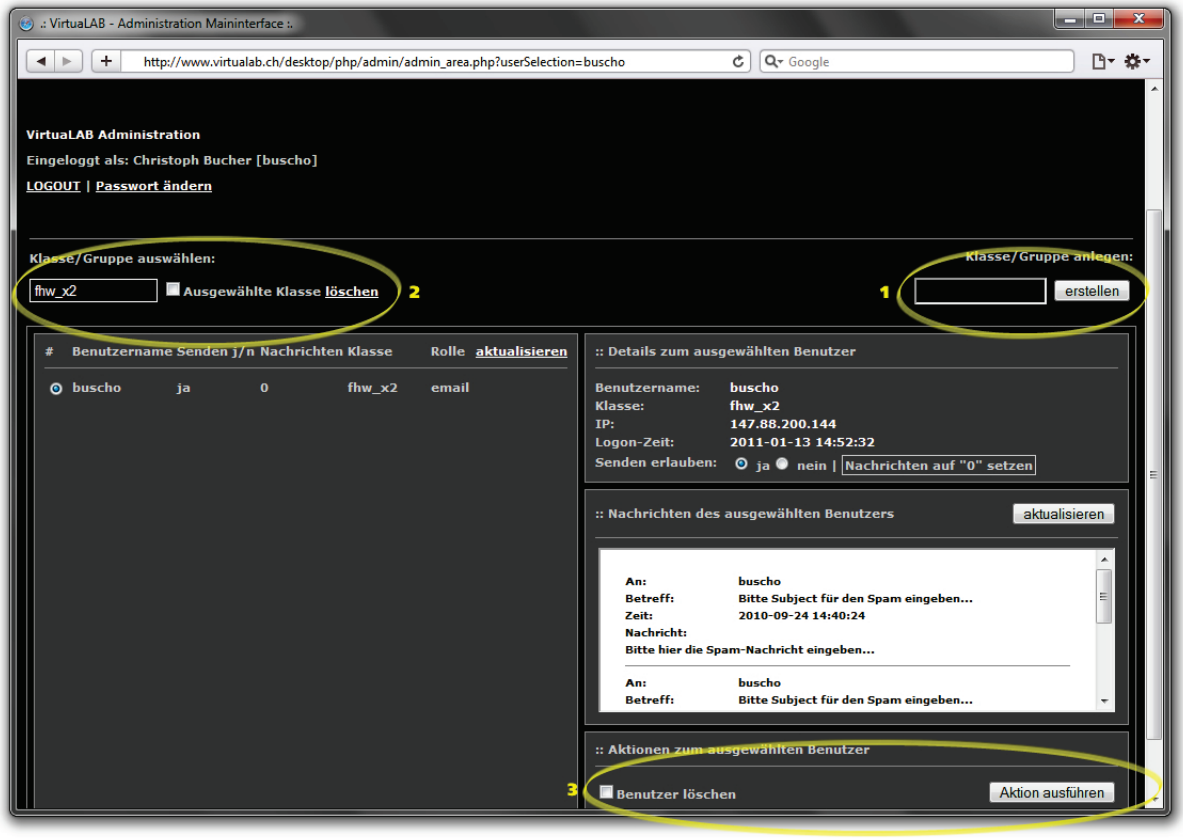

Abbildung 2-3: Administrationsinterface

Verwalten von Benutzern

In der linken Spalte des Administrationsinterfaces sind alle unter dem Namen der aktuell ausgewählten Klasse im System vorhandenen Studierenden ersichtlich. In Abbildung 2-3 ist zu sehen, dass momentan nur ein Studierender mit dem Benutzername *buscho* unter dem Klassennamen *fhw_x2* angemeldet ist. Durch Anwählen des Radio-Buttons links des Benutzernamens werden in der rechten Spalte des Administrationsinterfaces weitere Informationen über diesen Benutzer dargestellt.

Unter *Details zum ausgewählten Benutzer* sind Benutzername, Klassenname sowie IP-Adresse und Log-in-Zeit ersichtlich. Durch Anwählen des entsprechenden Radio-Buttons kann hier dem Benutzer explizit das Senden von E-Mail-Nachrichten (siehe 2.5.2) erlaubt, bzw. unterbunden werden. Durch Klicken auf *Nachrichten auf „0“ setzen*, wird der E-Mail-Nachrichtenzähler des Benutzers wieder auf null gesetzt. Standardmässig wird das Senden von E-Mails nach 15 verschickten Nachrichten automatisch unterbunden. Die Anzahl der bis dato versendeten Nachrichten ist in der Linken Spalte des Administrationsinterfaces ersichtlich.

Unter *Nachrichten des ausgewählten Benutzers* werden chronologisch alle durch den ausgewählten Benutzer versendeten E-Mail-Nachrichten angezeigt.

Unter *Aktionen zum ausgewählten Benutzer* (Markierung 3) ist es möglich, den aktuell gewählten Benutzer aus dem System zu löschen. Hierzu muss die Checkbox *Benutzer löschen* selektiert und die Schaltfläche *Aktion ausführen* geklickt werden. Dieser Schritt ist unter Umständen notwendig, falls sich

Studierende nicht korrekt aus der Simulationsumgebung abmelden. In diesem Falle bleibt nämlich der Benutzername im System bestehen und ein erneutes Anmelden unter demselben Namen ist nicht mehr möglich (siehe 2.4). Erst durch explizites Löschen des Benutzernamens aus dem System durch die Lehrperson wird dieser wieder verfügbar gemacht.

2.4 Einloggen in die Simulationsumgebung

Abbildung 2-4 zeigt die Login-Maske der Simulation „E-Mail“, wie sie sich präsentiert, nachdem Link 1 der Startseite (vergl. Abbildung 2-1) geklickt wurde. Die Login-Masken der Simulation „WWW“ (Desktopoberfläche des Opfers und Angreiferinterface) sehen gleich aus, wenn auch farblich differenziert.

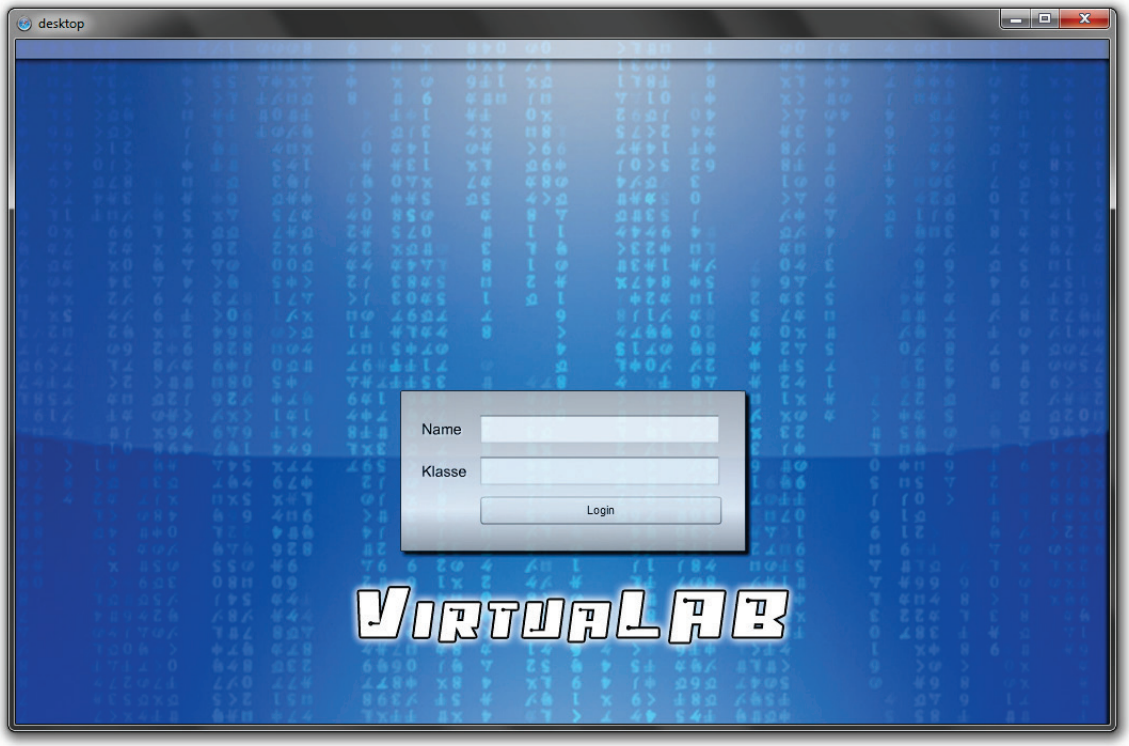

Abbildung 2-4: Login-Maske der Simulation

Für das Login kann von den Studierenden ein beliebiger Name verwendet werden – einzige Restriktion: Innerhalb einer Klasse darf der gleiche Name nicht mehrmals verwendet werden. Enthält der gewählte Benutzernamen Leerzeichen, so werden diese mit einem Unterstrich ersetzt. Grossbuchstaben werden zu Kleinbuchstaben gewandelt.

In das Feld *Klasse* muss ein gültiger Klassenname eingetragen werden – gültig bedeutet, dass dieser vorher von einer Lehrperson im Administrationsinterface angelegt wurde (siehe 2.3).

2.5 Simulation „E-Mail“

2.5.1 Sinn und Zweck

Die Simulation „E-Mail“ soll die Studierenden im Umgang mit E-Mails sensibilisieren. Hierzu wird Ihnen eine Desktopoberfläche zur Verfügung gestellt, welche – unter anderem – über ein E-Mail-Programm verfügt. In der Inbox des E-Mail-Programms sind bereits einige Nachrichten abgelegt. Ziel ist es nun, dass die Studierenden die E-Mails kritisch betrachten und anhand deren Inhalte und deren „Art“, wie sie verfasst und formuliert sind, als potentiell gefährlich oder als vertrauenswürdig einstufen können.

Einige E-Mails enthalten Dateianhänge, welche mit Malware verseucht sind. Werden diese Anhänge geöffnet, so hat dies negative Auswirkungen auf die simulierte Desktopoberfläche (z.B im Form von „Computerabstürzen“, Spam-Attacken, …).

Um einem solchen Befall durch Malware vorzubeugen, lässt sich in der Simulationsumgebung ein Anti-Viren-Programm aktivieren. Hiermit sollen den Studierenden die Möglichkeiten und Grenzen solcher Schutzprogramme bewusst gemacht werden – eine Anti-Viren-Software mag vielleicht einen infizierten Dateianhang erkennen, erweist sich jedoch bei einer Phishing-Attacke als nutzlos…

2.5.2 Beschreibung der simulierten Desktopoberfläche

Abbildung 2-5 zeigt die Desktopoberfläche der Simulation „E-Mail“ mit dem geöffneten E-Mail-Client und einer geöffneten Nachricht.

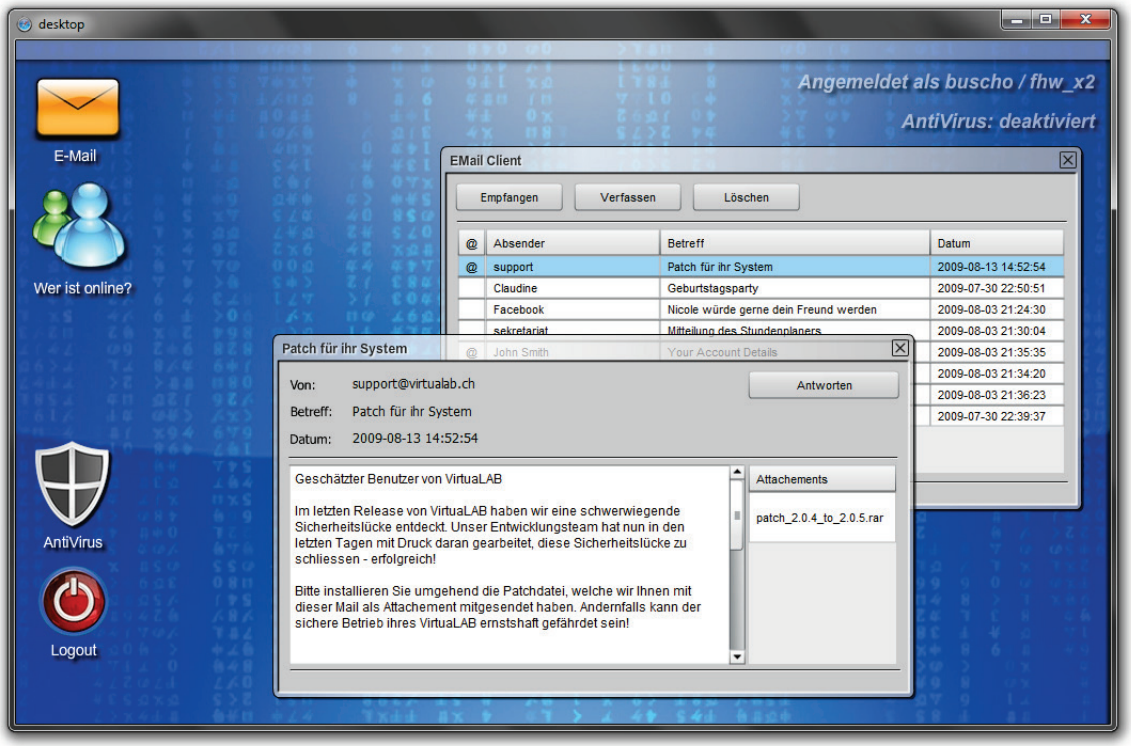

Abbildung 2-5: Desktopoberfläche Simulation „E-Mail“

Die Handhabung dieses „Desktops“ funktioniert analog einer „normalen“ Desktopoberfläche. Die Symbole lassen sich per Maus umherziehen und beliebig platzieren und ein Doppelklick auf ein Desktopsymbol startet die damit verbundene Anwendung.

Desktopsymbol „E-Mail“

Ein Doppelklick startet den E-Mail-Client. Durch klicken auf *Empfangen* werden neue Nachrichten heruntergeladen. Standardmässig werden acht vorkonfigurierte E-Mails heruntergeladen und in die Inbox abgelegt (siehe 2.5.1).

Studierende können sich aber auch gegenseitig eigene E-Mail-Nachrichten schicken (Schaltfläche *Verfassen*). Nachrichten können nur zwischen Benutzer, welche unter dem gleichen Klassennamen angemeldet sind, ausgetauscht werden. Als Empfänger muss der Login-Name eines anderen Studierenden angegeben werden.

Durch einen Klick auf *Löschen* kann eine markierte Nachricht aus dem Posteingang entfernt werden.

Ein Doppelklick auf eine Nachricht in der Inbox öffnet selbige – in Abbildung 2-5 ist z.B. eine Nachricht mit dem Betreff *Patch für Ihr System* geöffnet. In der rechten Spalte der geöffneten E-Mail sind eventuell vorhandene Dateianhänge (z.B. *patch_2.0.4_2.0.5.rar*) gelistet. Diese lassen sich ebenfalls durch einen Doppelklick öffnen und haben – je nach dem – einen „nicht erwünschten“ Effekt auf die simulierte Desktopoberfläche.

Desktopsymbol „Wer ist online?“

Ein Doppelklick startet ein kleines Programm, welches in einer Liste alle unter dem gleichen Klassennamen des eingeloggten Benutzers am System angemeldeten Studierenden anzeigt. Durch einen Doppelklick auf einen Namen in der Liste lässt sich direkt eine neue E-Mail-Nachricht mit dem entsprechenden Empfänger verfassen.

Desktopsymbol „AntiVirus“

Ein Doppelklick auf dieses Symbol schaltet das Anti-Viren-Programm ein oder wieder aus. Bei ausgeschaltetem Programm ist das Symbol *grau* und oben rechts auf der simulierten Desktopoberfläche ist der Hinweis *„AntiVirus: deaktiviert“* ersichtlich. Bei eingeschaltetem Anti-Viren-Programm erscheint das Symbol *blau* und der Hinweis lautet *„AntiVirus: aktiviert“*.

Desktopsymbol „Logout“

Um sich korrekt von der Simulation abzumelden, sollte dieses Desktopsymbol doppelgeklickt werden. Es öffnet sich daraufhin ein kleines Dialogfenster, welches nachfragt, ob man sich wirklich abmelden will – diese Meldung ist entsprechend mit einem Klick auf *OK* zu bestätigen (oder mit *Abbrechen*, falls man doch noch weiterarbeiten möchte).

Wird statt dieses regulären Abmeldevorgangs einfach das Browserfenster, in welchem die simulierte Desktopoberfläche läuft, geschlossen, so wird der Benutzername nicht ordnungsgemäss aus der Datenbank des Systems gelöscht. Ein erneutes Anmelden unter demselben Benutzernamen ist dann nicht mehr möglich, bis eine Lehrperson denselben explizit im Administrationsinterface gelöscht hat (siehe 2.3.2).

2.5.3 Spezielles

Die Simulationsumgebung ist standardmässig daher konfiguriert, dass die Studierenden maximal 15 Nachrichten versenden können. Wird diese Anzahl überschritten, so wird ihnen automatisch eine Warnmeldung angezeigt, wenn sie versuchen, eine weitere E-Mail zu verschicken. Eine Lehrperson hat dann die Möglichkeit, den E-Mail-Nachrichtenzähler eines betroffenen Studierenden wieder auf null zu setzen, damit dieser erneut Nachrichten versenden kann (siehe 2.3.2).

2.6 Simulation „WWW“

2.6.1 Sinn und Zweck

Die Simulation „WWW“ solle die Studierenden auf potenzielle Gefahren, denen man beim Surfen im Internet ausgesetzt ist, sensibilisieren. Es wird ihnen aufgezeigt, welche Möglichkeiten einem Angreifer offen stehen, wenn er – durch Infizieren mit entsprechender Malware – die Kontrolle über den Rechner eines Opfers erlangt.

Hierzu werden in der Simulation „WWW“ zum einen eine Desktopoberfläche zur Verfügung gestellt, die den Computer des (ahnungslosen) Opfers darstellt und auf dessen Desktop sich die Auswirkungen diverser Malware-Attacken direkt verfolgen lassen. Zum anderen beinhaltet die Simulation „WWW“ ein Angreiferinterface, mit Hilfe dessen der Angreifer sein Opfer (es können auch mehrere sein) kontrollieren kann, indem er verschiedene Arten von Malware auf den Rechner des Opfers lädt und somit z.B. dessen Tastatureingaben mitliest, in dessen Namen E-Mail-Spam versendet oder gar dessen Computer zum Absturz bringt.

2.6.2 Beschreibung der simulierten Desktopoberfläche

Abbildung 2-6 zeigt die Desktopoberfläche des Opfers, also des infizierten Rechners. Die grundsätzliche Funktionsweise ist derjenigen der Simulation „E-Mail“ identisch (vergl. 2.5.2). Die Unterschiede werden im Folgenden beschrieben.

Desktopsymbole „E-Mail“, „Wer ist online?“, „AntiVirus“ und „Logout“

Die Funktion hinter diesen Symbolen entspricht der Simulation „E-Mail“ (vergl. 2.5.2) und wird an dieser Stelle nicht nochmals erwähnt. Einziger kleiner Unterschied: Standardmässig sind keine vorbereiteten E-Mail-Nachrichten im Posteingang vorhanden.

Desktopsymbol „FlashPlayer_Update.exe“

Das Szenario der Simulation „WWW“ sieht vor, dass sich ein (ahnungsloses) Opfer auf einer Webseite einen Film anschauen will, beim Besuch dieser Webseite jedoch dazu angehalten wird, sich das neueste Update für den FlashPlayer herunterzuladen und zu installieren.

Gleich nach dem Login ist die Desktopoberfläche des Opfers noch „sauber“, also noch nicht mit Malware infiziert. Die Studierenden schlüpfen nun in die Rolle des (ahnungslosen Opfers), welches soeben die im vorherigen Szenario beschriebene Update-Datei auf den Desktop heruntergeladen hat. Durch einen Doppelklick auf das Desktopsymbol wird nun vermeintlich der Installationsprozess des Updates gestartet – doch statt eines Installationsvorgangs erscheint bloss eine Meldung, dass etwas schief gelaufen

ist… und schon ist die simulierte Desktopoberfläche des Opfers mit Malware infiziert und kann fortan durch den Angreifer kontrolliert und manipuliert werden.

Desktopsymbol „SimplePad Editor“

Durch einen Doppelklick auf dieses Symbol wird ein kleines Programm geöffnet, das einen Texteditor simulieren soll. Das Programm hat weiter keine Funktion, als dass ein paar Zeilen Text geschrieben werden können – es ist jedoch notwendig, damit der Effekt der „Keylogger-Malware“ (siehe 2.6.3) demonstriert werden kann.

Statusbereich über den Grad der Malware-Infektion

Im unteren rechten Bereich der simulierten Desktopoberfläche des Opfers ist ein kleines Statusfenster ersichtlich. Es lässt sich per Drag&Drop mit der Maus an eine beliebige Position des Bildschirms verschieben. Das Statusfenster gibt Auskunft, ob der Rechner aktuell „sauber“ oder „infiziert“ ist und – im zweiten Falle – welche Malware-Funktion gerade aktiv („on“) oder inaktiv („off“) ist. Dies kann vom Angreifer entsprechend über das Angreiferinterface gesteuert werden.

Abbildung 2-6: Desktopoberfläche Simulation „WWW“

2.6.3 Beschreibung des simulierten Angreiferinterfaces

Abbildung 2-7 zeigt die Oberfläche des Angreiferinterfaces, mit Hilfe dessen der Angreifer ein oder mehrere infizierte Opferrechner kontrollieren kann. Angreifer wie auch Opfer müssen unter dem gleichen Klassennamen in der Simulation angemeldet sein, damit eine Kontrolle möglich ist. Zudem muss das Opfer „seinen Rechner“ erst infizieren (siehe 2.6.2).

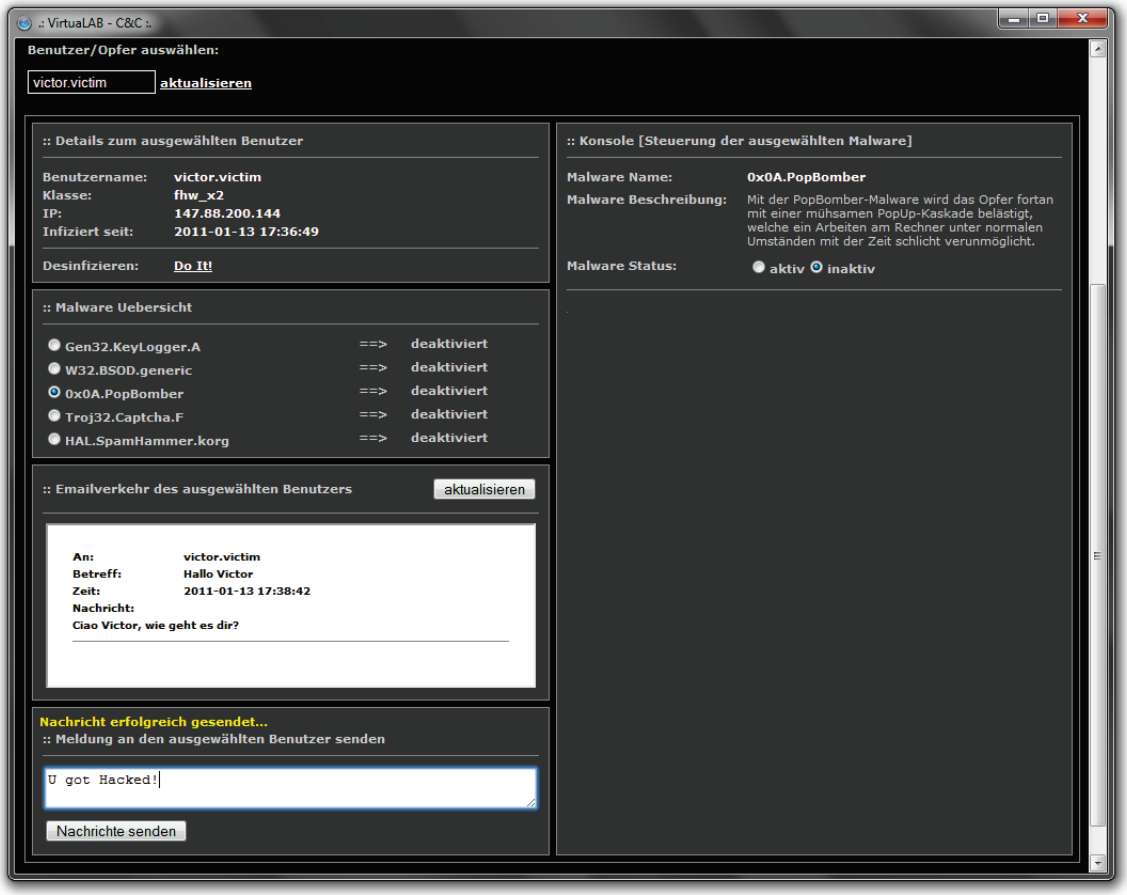

Abbildung 2-7: Oberfläche des Angreifinterfaces

In der DropDown-Box oben links werden alle momentan infizierten Opfer angezeigt. Durch klicken auf den Link *aktualisieren* werden in der Zwischenzeit neu infizierte Opfer frisch in die Liste aufgenommen. Um den Rechner eines Opfers nun zu kontrollieren, wählt der Angreifer den Benutzernamen des Opfers aus der DropDown-Box aus – das Angreiferinterface aktualisiert sich daraufhin automatisch mit den Daten des ausgewählten Opfers.

Details zum ausgewählten Benutzer

Hier werden Benutzer- und Klassennamen sowie IP-Adresse und Infektionszeit des selektierten Opfers angezeigt. Durch einen Klick auf den Link *Do It!* kann der Angreifer das Opfer wieder vollständig desinfizieren. Er hat daraufhin keine Möglichkeit mehr, über den Rechner des Opfers Gewalt zu erlangen – ausser das Opfer infiziert sich erneut durch doppelklicken der Update-Datei (siehe 2.6.2).

Malware Übersicht und Konsole [Steuerung der ausgewählten Malware]

In der *Malware Übersicht* (linke Spalte) werden die Malware-Typen, die dem Angreifer zur Verfügung stehen, aufgelistet. Wählt der Angreifer eine Malware mit dem Radio-Button aus, so werden in der *Konsole [Steuerung der ausgewählten Malware]* (rechte Spalte) die Details und – falls vorhanden – die Optionen zu weiteren Konfigurationsmöglichkeiten von dieser dargestellt. Jedem Typ Malware gemeinsam ist, dass er sich durch anwählen des Radio-Buttons *aktiv* oder *inaktiv* auf dem Opferrechner entspre-

chend „installieren“, bzw. „deinstallieren“ lässt. Die fünf zur Verfügung stehenden Malware-Typen in der Übersicht:

Gen32.KeyLogger.A: Diese Malware zeichnet die Tastaturanschläge auf, welche das Opfer in der Anwendung *SimplePad Editor* eingibt. Um diesen Effekt zu beobachten, muss auf dem Rechner des Opfers also der *SimplePad Editor* gestartet sein (siehe 2.6.2). Zusätzlich kann mit dieser Malware ein Logout des Opfers aus der simulierten Desktopoberfläche erzwungen werden. Das Opfer logt sich daraufhin wieder ein und die Login-Daten (Benutzername und Passwort) werden dem Angreifer im Angreiferinterface präsentiert.

W32.BSOD.generic: Wird diese Malware aktiviert, so “stürzt” die simulierte Desktopumgebung des Opfers ständig ab – ein normales Arbeiten ist somit nicht mehr möglich.

0x0A.PopBomber: Diese Malware verursacht auf dem Rechner des Opfers eine Kaskade von PopUp-Fenstern, welche nicht mehr aufhört, ehe die Malware wieder auf “inaktiv” gesetzt wird.

***Troj32.Captcha.F*:** Bei Aktivierung dieser Malware wird dem Opfer dessen Bildschirm gesperrt und stattdessen ein Captcha eingeblendet. Der Bildschirm des Opfers wird erst wieder freigegeben, nachdem dieses das Captcha korrekt gelöst hat. Die vom Captcha angezeigten Zeichen lassen sich dabei vom Angreifer frei konfigurieren.

***HAL.SpamHammer.korg*:** Diese Malware dient dem Angreifer dazu, im Namen seines ausgewählten Opfers E-Mail-Spamnachrichten zu versenden. Betreff und Inhalt der Spamnachricht können vom Angreifer bestimmt werden. Jedesmal auf Knopfdruck des Angreifers wird nun unter dem Benutzernamen des Opfers eine E-Mail-Spamnachricht an alle anderen, unter dem gleichen Klassennamen angemeldeten Benutzer versendet.

Emailverkehr des ausgewählten Benutzers

Hier wird der gesamte E-Mail-Nachrichtenverkehr des Opfers chronologisch dargestellt und kann vom Angreifer 1:1 mitgelesen werden.

Meldung an den ausgewählten Benutzer senden

Dieser Bereich ermöglicht es dem Angreifer Nachrichten direkt auf den Desktop des Opfers zu senden. Die Nachrichten erscheinen in Form von kleinen Dialogfenstern und müssen vom Opfer explizit wieder geschlossen werden.

2.6.4 Spezielles

Wie auch für die Simulation „E-Mail“ gilt auch für die Simulation „WWW“ das standardmässige Limit von 15 Nachrichten, welche die Studierenden versenden können, ehe das Verschicken blockiert und eine entsprechende Meldung angezeigt wird (vergl. 2.5.3)

3 Technische Informationen zur Simulation

3.1 Überblick über die Architektur

Abbildung 3-1 stellt die Architektur der Simulationsumgebung in einer vereinfachten Weise dar.

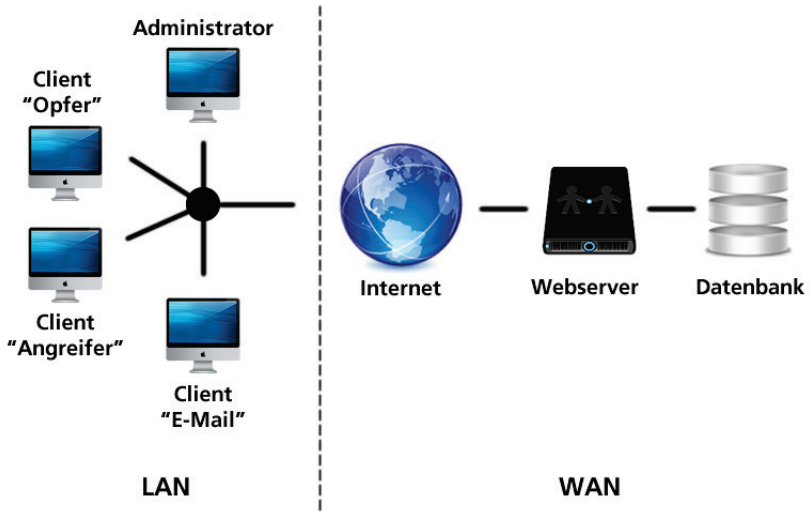

Abbildung 3-1: Architektur der Simulationsumgebung

Die linke Seite (LAN) stellt ein Schulzimmer dar, in welchem die Simulation im Unterricht eingesetzt wird. Die einzelnen Arbeitsstationen sind untereinander vernetzt und haben allesamt Zugang zum Internet (WAN).

Auf den einzelnen Arbeitsstationen können im Webbrowser die einzelnen Simulationsumgebungen („E-Mail“, „WWW“, Administrations- oder Angreiferinterface) gestartet werden. Alle dazu notwendigen Daten (es handelt sich um „normale“ Webseiten) sind auf dem Webserver gespeichert und werden von dort direkt in den Browser geladen und angezeigt – auf Seiten der Clients braucht keine spezielle Software installiert zu werden (siehe 3.2.2).

Die Login-Daten der einzelnen Benutzer (Benutzername und Klassename) werden in der Datenbank hinterlegt. Meldet sich ein Benutzer wieder von der Simulation ab (vergl. 2.5.2), so werden diese Daten wieder aus der Datenbank gelöscht. Meldet sich ein Benutzer nicht korrekt ab, so verbleiben seine Daten in der Datenbank, bis ein Administrator (Lehrperson) diese explizit löscht, längstens aber bis zur folgenden Nacht um 03:00h – um diese Zeit wird täglich ein Skript ausgeführt, welches alle noch angemeldeten Benutzer aus dem System entfernt. Die Login-Daten von registrierten Benutzern (Lehrpersonen) bleiben jedoch dauerhaft in der Datenbank gespeichert.

Sämtlicher Datenaustausch zwischen den einzelnen Simulationsumgebungen erfolgt ebenfalls über den Webserver und die Datenbank – z.B. die zwischen den Studierenden versendeten E-Mail-Nachrichten werden ebenfalls temporär in der Datenbank abgelegt.

3.2 Systemanforderungen

3.2.1 Seite Server (WAN)

Die Systemanforderungen auf der Server Seite sind für den Betrieb und die Anwendung der Simulation im Unterricht nicht relevant, da diese Infrastruktur vom Betreiber der Simulation zur Verfügung gestellt und unterhalten wird. Der Vollständigkeit halber sind an dieser Stelle trotzdem einige grundlege technische Hinweise notiert.

Folgende Systemanforderungen sind auf Seite des Servers zu erfüllen

- Beliebiger Webserver mit Unterstützung der Skriptsprache PHP (ab Version 5)
- MySQL Datenbank (ab Version 4.1.25)

3.2.2 Seite Client (LAN)

Folgende Systemanforderungen sind auf Seiten der Clients zu beachten, resp. zu erfüllen:

- Ständige Verbindung zum Internet – ein Offlinebetrieb ist nicht möglich
- Es gelten keine besonderen Anforderungen an das Betriebssystem (getestet auf aktuellen Versionen von Linux, Mac OS X und Windows)
- Eine Bildschirmauflösung von mindestens 1024x768 Pixel ist zu empfehlen
- Die Simulationsumgebung wird vollständig über den Webbrowser bedient – sie wurde erfolgreich auf den aktuellen Versionen von Firefox, Safari, Opera und Internet Explorer getestet
- Zur Betrachtung der Desktopoberflächen der Simulation „E-Mail“ und „WWW“ muss im Browser das FlasPalyer-Plugin (ab Version 10) installiert sein
- Das Administrations- sowie das Angreiferinterface können auch ohne FlashPalyer-Plugin betrachtet und verwendet werden (z.B. über den Browser eines iPhones)

3.3 Programmiertechnische Aspekte

3.3.1 Allgemeines

Grundsätzlich erfolgt der Informations- und Datenaustausch zwischen den einzelnen Komponenten (Administrations- und Angreiferinterface und den Simulationsumgebungen „E-Mail“ und „WWW“) über die MySQL Datenbank. Für den Zugriff auf die Datenbank wird die Skriptsprache PHP verwendet.

Jede gestartet Komponente der Simulationsumgebung registriert sich dazu mit den verwendeten Login-Daten (Benutzername und Klasse) in der Datenbank und kann so eindeutig identifiziert werden. Eine Komponente kann auf diese Weise gezielt Daten (z.B. eine neue E-Mail-Nachricht) an eine andere Komponente adressiert in der Datenbank abspeichern.

Sämtliche Komponenten überprüfen nun fortlaufend in definierten Abständen, ob in der Datenbank neue, an sie adressierte Daten vorhanden sind. Ist dies der Fall, so werden diese Daten interpretiert und

eine entsprechende Aktion ausgelöst (z.B. das Ablegen einer neuen Nachricht im Posteingang oder auch das Installieren oder Aktivieren einer Malware).

3.3.2 Desktopoberflächen der Simulation „E-Mail“ und „WWW“

Die grafischen Desktopoberflächen der Simulationsumgebungen wurden vollständig mit dem Programm *Adobe Flash Professional CS 4* erstellt. Entsprechend muss zum Betrachten dieser sogenannten Flash-Filme das FlashPlayer-Plugin im Browser installiert sein.

Zum Speichern und Abrufen von Daten in und von der Datenbank übergibt ein Flash-Film diese Daten an PHP-Skripte, welche sie dann mit den entsprechenden SQL-Befehlen in der Datenbank ablegen, bzw. die entsprechende Datenbankabfrage tätigen, und das Resultat zurück an den aufrufenden Flash-Film senden, der sie dann wieder interpretieren und darstellen kann.

3.3.3 Administrations- und Angreiferinterface

Das Administrations- und Angreiferinterface sind in der Skriptsprache PHP programmiert. Sie enthalten entsprechend programmierte Funktionen, mit Hilfe derer sie direkt mit der Datenbank kommunizieren und Daten abspeichern oder die für eine bestimmte Aktion benötigten Daten besorgen oder abrufen können.

Abbildungsverzeichnis