)SCIP(

scip ag

Contents

1. Editorial

Whitehate

Für Aussenstehende klingt der Begriff "Whitehate" nach einer rassistischen Tendenz. Tatsächlich handelt es sich hier um einen alten Ausdruck, der von Kriminellen im "Untergrund" genutzt wird, um ihren Unmut über professionelle Sicherheitsexperten zum Ausdruck zu bringen. Die Blackhat-Hacker zeigen damit ihren Hass gegenüber den Whitehat-Hackern.

Ich habe mich nie als Blackhat verstanden, denn für mich stand beim Thema Informationssicherheit stets der wissenschaftliche und soziale Aspekt im Mittelpunkt. Es ist unvermeidbar, dass wir uns heutzutage in einer Informationsgesellschaft wiederfinden und Informationssicherheit deshalb zu einem zentralen Aspekt des Zusammenlebens geworden ist. Ethische und moralische Tugenden sollen deshalb auch auf virtueller Ebene verteidigt werden.

Darum habe ich sehr früh davon abgesehen, mit einem Pseudonym aufzutreten. Stattdessen habe ich von Beginn weg Artikel unter meinem echten Namen publiziert. Ich wollte damit die Grundlage schaffen, um irgendwann professionell im Bereich der Informationssicherheit arbeiten zu können. Im Jahr 2000 habe ich das dann auch geschafft, als ich beim deutschen Unternehmen Biodata Information Technology AG als IT Security Expert anfangen konnte.

Schon damals wurde ich in diversen Foren als Verräter dargestellt, der sich für Geld prostituiert. Zudem sei mein Wissen mangelhafter Natur und damit sowieso bewiesen, dass sogenannte "professionelle Computersicherheit" nichts taugt. Ich kann diese Argumentation bis heute nicht nachvollziehen.

Als viel schwerwiegender verstehe ich hingegen das offensichtlich zur Schau getragene Unwissen, wie Informationssicherheit beschaffen ist. Viele Kiddies denken, dass Coding und Exploiting die Hauptpfeiler dieses Themengebiets sind. Tatsächlich ist es bedeutend vielschichtiger und komplexer. Wer nur auf diesen beiden Gebieten bewandert ist, wird in unserer Firma noch nicht einmal zu einem Vorstellungsgespräch eingeladen.

Unsere Kunden erwarten, dass wir sämtliche Aspekte der Informationssicherheit verstehen können. Dazu gehört beispielsweise auch das in technischen Kreisen gerne vernachlässigte Thema Risikomanagement. Bevor man über Exploits und Patches spricht, sollte man über Bedrohungen und Risiken reden. Denn das Hauptziel der Kunden ist stets das Eliminieren geschäftsbeinflussender Risiken und somit der gezielte und effiziente Einsatz der aufzuwendenen Ressourcen.

Ein gutes Beispiel, warum ein Blackhat nicht einfach die Arbeit eines Whitehat machen kann, findet sich im Bereich der Backdoor Tests. Durch das Entwickeln einer kundenspezifischen Malware soll ein möglichst realistischer Angriff durchgespielt werden. Durch diesen wird es möglich, sämtliche Facetten der etablierten Sicherheitsmassnahmen betrachten zu können.

Ein Blackhat wird in den meisten Fällen eine Malware programmieren, um seiner Experimentierfreudigkeit und Kreativität freien Lauf zu lassen. Ob und inwiefern etwas bei der Ausführung mal nicht reibungslos funktioniert, ist eher zweitrangig, sofern es überhaupt funktioniert. Bei einer professionellen Sicherheitsüberprüfung sind jedoch ganz andere Anforderungen gegeben.

Hier geht es darum, ein Maximum an Zuverlässigkeit, Nachvollziehbarkeit und Transparenz zu erreichen. Die Entwicklungs-

Phase ist in den meisten Fällen schnell abgeschlossen (üblicherweise 2-3 Manntage). Überproportional viel Aufwand wird hingegen in das Testing gesteckt (im Extremfall bis zu 30 Manntagen). Schliesslich wird man mit der Malware eine produktive Umgebung infiltrieren und dabei darf ja nichts schief gehen. Zudem muss zu jedem Zeitpunkt klar ausgewiesen werden können, welche Systeme infiziert sind und wie weit die Infizierung fortgeschritten ist. Im Notfall muss unverzüglich eine Desinfektion stattfinden können. Fremd-Infektionen von Systemen anderer Firmen sind dabei genauso zu verhindern, wie ein Verlust der Kommunikationsmöglichkeit mit dem C&C-Server. Diese Funktionalitäten einzubringen erfordert zusätzlichen Aufwand.

Erweiterte Anforderungen dieser Art gibt es bei allen Projekten, egal ob es sich nun um Backdooring, Exploiting oder Auditing handelt. In der Geschäftswelt in produktiver Weise und mit Verlässlichkeit zu agieren, ist bedeutend schwieriger, als sich die meisten Hobby-Hacker vorstellen. Denn da gibt es immer jemanden, bei dem man sich für seine Fehler rechtfertigen muss. Und im schlimmsten Fall hat dies gar finanzielle oder juristische Auswirkungen. Denn wer übernimmt die Kosten, wenn die Malware keine eigenständige Desinfektion mehr umsetzen kann und stattdessen auf 120'000 Rechnern in verschiedenen Ländern eine manuelle Säuberung stattzufinden hat?

Die Zeiten ändern sich wohl nie und so habe ich gerade vor einigen Wochen eine Foren-Diskussion mitgekriegt, in der meine Arbeit mit "Whitehate" abgespiesen wurde. Schade, dass die Schreiberlinge sich nicht die Mühe gemacht haben, meinen gesamten Artikel zu lesen. Weil dann hätten sie ihre Fehlbarkeit bemerken müssen. Es zeugt nicht gerade von Professionalität der selbsternannten "Blackhats", wenn sie sich nicht einmal die Mühe machen, die einfachen Fakten zu prüfen. So jemanden würde ich ebenfalls nie zu einem Vorstellungsgespräch einladen wollen.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 28. November 2011

2. scip AG Informationen

2.1 Penetration Test

Das Ziel unserer Dienstleistung Penetration Test ist die Identifikation vorhandener Sicherheitslücken sowie die Definierung der Tragweite dadurch möglicher erfolgreicher Attacken durch Angreifer.

Der Kunde hat ein abgesichertes System vorliegen, das er mittels Ethical Hacking untersucht haben möchte. Um eine wissenschaftliche und wirtschaftliche Optimierung des Auftrags erreichen zu können, wird eine Whitebox-Analyse empfohlen: Der Kunde legt nach Möglichkeiten sämtliche Details zum Zielobjekt offen (IP-Adressen etc.). Somit kann unser Red Team auf eine langwierige Datensammlung verzichten und stattdessen das Expertenwissen auf die Fachgebiete fokussieren.

Das Umsetzen von Penetration Tests basiert zu grossen Teilen auf der systematischen Vorgehensweise, wie sie im Buch „Die Kunst des Penetration Testing“ unseres Herrn Marc Ruef dokumentiert wurde.

- Scanning: Identifizieren von möglichen Angriffsflächen.
- Auswertung: Eingrenzen potentieller Angriffsvektoren, die sich im Rahmen eines konkreten Angriffsszenarios angehen lassen.
- Exploiting: Zielgerichtetes Ausnutzen ausgemachter Sicherheitslücken (Proof-of-Concept).

Ein Penetration Test lässt eine konkrete und verlässliche Aussage bezüglich der existenten Sicherheit eines Systems zu. Die Ausnutzbarkeit von Schwachstellen sowie die Tragweite erfolgreicher Attacken können exakt bestimmt werden, wodurch sich weitere Schritte wie z.B. Risiken akzeptieren oder Gegenmassnahmen einleiten, planen lassen.

Dank unserem ausgewiesenen Expertenwissen kann die scip AG auf eine Vielzahl von Penetration Tests auf unterschiedliche Plattformen, Applikationen und Lösungen zurückblicken.

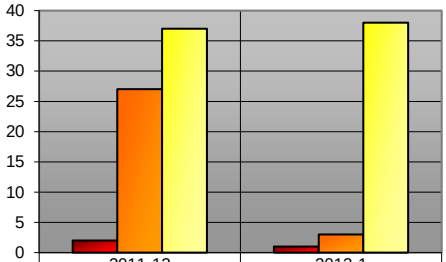
Zählen auch Sie auf uns!
http://www.scip.ch/?firma.referenzenalle

Zögern Sie nicht und kontaktieren Sie unseren Herrn Simon Zumstein unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an simon.zumstein@scip.ch.

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter http://www.scip.ch/?vuldb einsehbar.

Das Dienstleistungspaket VulDB Alert System liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind: http://www.scip.ch/?vuldb.alertsystem



	2011-12	2012-1
sehr kritisch	2	1
kritisch	27	3
problematisch	37	38

Inhalt

3.1 McAfee Security-as-a-Service myCIOScn.dll MyCioScan.Scan.ShowReport() Command Injection

Risiko: sehr kritisch
Datum: 12.01.2012
VulDB: http://www.scip.ch/?vuldb.4552

Es wurde eine sehr kritische Schwachstelle in McAfee Security-as-a-Service entdeckt. Diese betrifft die Funktion MyCioScan.Scan.ShowReport() in der Bibliothek myCIOScn.dll. Durch die Manipulation mit einer unbekannten Eingabe kann eine Command Injection-Schwachstelle ausgenutzt werden. Die genauen Auswirkungen eines erfolgreichen Angriffs sind bisher nicht bekannt.

Es sind keine Informationen bezüglich Gegenmassnahmen bekannt.

3.2 Microsoft Windows Ntdll.dll unbekannte Schwachstelle

Risiko: kritisch
Datum: 10.01.2012
VulDB: http://www.scip.ch/?vuldb.4546

Es wurde eine kritische Schwachstelle in Microsoft Windows entdeckt. Diese betrifft eine unbekannte Funktion in der Bibliothek Ntdll.dll. Es sind keine weiteren technischen Informationen bekannt. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Als Gegenmassnahme wird das Einspielen des entsprechenden Patches empfohlen.

3.3 Apache Struts ParameterInterceptor Directory Traversal

Risiko: kritisch
Datum: 03.01.2012
VulDB: http://www.scip.ch/?vuldb.4513

Es wurde eine kritische Schwachstelle in Apache Struts bis 2.3.1.1 entdeckt. Diese betrifft eine unbekannte Funktion der Komponente ParameterInterceptor. Durch die Manipulation mit der Eingabe ../../ kann eine Directory Traversal-Schwachstelle ausgenutzt werden. Dadurch lässt sich erweiterte Dateizugriffe. Dies hat Auswirkungen auf Integrität und Verfügbarkeit.

Als Gegenmassnahme wird das Aktualisieren auf eine neue Version empfohlen. Ein Upgrade auf die Version 2.3.1.1 vermag dieses Problem zusätzlich zu lösen. Das Erscheinen einer

Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Apache hat demnach sofort reagiert.

3.4 Apache Struts CookieInterceptor Command Injection

Risiko: kritisch
Datum: 03.01.2012
VulDB: http://www.scip.ch/?vuldb.4512

Es wurde eine kritische Schwachstelle in Apache Struts bis 2.3.1.1 entdeckt. Diese betrifft eine unbekannte Funktion der Komponente CookieInterceptor. Durch die Manipulation mit einer unbekannten Eingabe kann eine Command Injection-Schwachstelle ausgenutzt werden. Dadurch lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Als Gegenmassnahme wird das Aktualisieren auf eine neue Version empfohlen. Ein Upgrade auf die Version 2.3.1.1 vermag dieses Problem zusätzlich zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Apache hat demnach sofort reagiert.

3.5 Microsoft .NET Framework Username Parser erweiterte Zugriffsrechte

Risiko: kritisch
Datum: 29.12.2011
VulDB: http://www.scip.ch/?vuldb.4508

Es wurde eine kritische Schwachstelle in Microsoft .NET Framework bis 4.0 entdeckt. Diese betrifft eine unbekannte Funktion der Komponente Username Parser. Durch die Manipulation mit einer unbekannten Eingabe kann eine erweiterte Zugriffsrechte-Schwachstelle ausgenutzt werden. Dadurch lässt sich Authentisierung umgehen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Als Gegenmassnahme wird das Einspielen des entsprechenden Patches empfohlen. Die Schwachstelle lässt sich zusätzlich durch das Einspielen eines Patches beheben. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Microsoft hat demnach sofort reagiert.

3.6 Microsoft .NET Framework ASP.NET Hash Denial of Service

Risiko: kritisch
Datum: 28.12.2011
VulDB: http://www.scip.ch/?vuldb.4506

Es wurde eine kritische Schwachstelle in Microsoft .NET Framework bis 4.0 entdeckt. Diese betrifft eine unbekannte Funktion der Komponente ASP.NET Hash. Durch die Manipulation mit einer unbekannten Eingabe kann eine Denial of Service-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Verfügbarkeit.

Als Gegenmassnahme wird das Einspielen des entsprechenden Patches empfohlen. Das Erscheinen einer Gegenmassnahme geschah 1 Tage nach der Veröffentlichung der Schwachstelle. Microsoft hat demnach unverzüglich reagiert.

3.7 FreeBSD telnet/libtelnet/encrypt.c encrypt_keyid() Pufferüberlauf

Risiko: sehr kritisch
Datum: 23.12.2011
VulDB: http://www.scip.ch/?vuldb.4504

Es wurde eine sehr kritische Schwachstelle in FreeBSD bis 9.0 entdeckt. Diese betrifft die Funktion encrypt_keyid() der Komponente telnet/libtelnet/encrypt.c. Durch die Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dadurch lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Als Gegenmassnahme wird das Aktualisieren auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Der Hersteller hat demnach sofort reagiert.

3.8 IBM Lotus Domino RPC Authentication Denial of Service

Risiko: kritisch
Datum: 21.12.2011
VulDB: http://www.scip.ch/?vuldb.4501

Es wurde eine kritische Schwachstelle in IBM Lotus Domino bis 8.5.2 entdeckt. Diese betrifft eine unbekannte Funktion der Komponente RPC Authentication. Durch die Manipulation mit einer unbekannten Eingabe kann eine Denial of Service-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Verfügbarkeit.

Als Gegenmassnahme wird das Aktualisieren auf eine neue Version empfohlen. Ein Upgrade auf die Version 8.5.2 Fix Pack 4 vermag dieses Problem zusätzlich zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. IBM hat demnach sofort reagiert.

3.9 Mozilla Firefox DOM Pufferüberlauf

Risiko: kritisch
Datum: 20.12.2011
VulDB: http://www.scip.ch/?vuldb.4497

Es wurde eine kritische Schwachstelle in Mozilla Firefox 8.0 for Mac entdeckt. Diese betrifft eine unbekannte Funktion der Komponente DOM. Durch die Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dadurch lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Als Gegenmassnahme wird das Aktualisieren auf eine neue Version empfohlen. Ein Upgrade auf die Version 9.0 vermag dieses Problem zusätzlich zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Mozilla hat demnach sofort reagiert.

3.10 Mozilla Firefox SVG Element Handler DOMAttrModified Pufferüberlauf

Risiko: kritisch
Datum: 20.12.2011
VulDB: http://www.scip.ch/?vuldb.4495

Es wurde eine kritische Schwachstelle in Mozilla Firefox 8.0 entdeckt. Diese betrifft die Funktion DOMAttrModified der Komponente SVG Element Handler. Durch die Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dadurch lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Als Gegenmassnahme wird das Aktualisieren auf eine neue Version empfohlen. Ein Upgrade auf die Version 9.0 vermag dieses Problem zusätzlich zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Mozilla hat demnach sofort reagiert.

3.11 Mozilla Firefox YARR Regular Expression Library erweiterte Rechte

Risiko: kritisch
Datum: 20.12.2011
VulDB: http://www.scip.ch/?vuldb.4493

Es wurde eine kritische Schwachstelle in Mozilla Firefox 8.0 entdeckt. Diese betrifft eine unbekannte Funktion der Komponente YARR Regular Expression Library. Durch die Manipulation mit einer unbekannten Eingabe kann eine erweiterte Rechte-Schwachstelle ausgenutzt werden. Dadurch lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Als Gegenmassnahme wird das Aktualisieren auf eine neue Version empfohlen. Ein Upgrade auf die Version 9.0 vermag dieses Problem zusätzlich zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Mozilla hat demnach sofort reagiert.

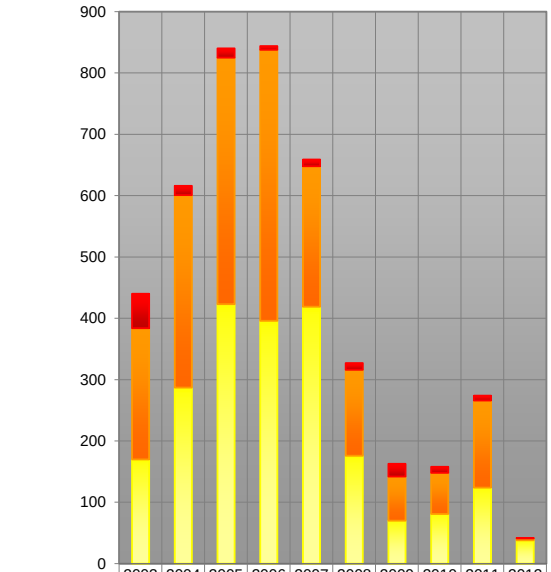
4. Statistiken Verletzbarkeiten

Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.

http://www.scip.ch/?vuldb

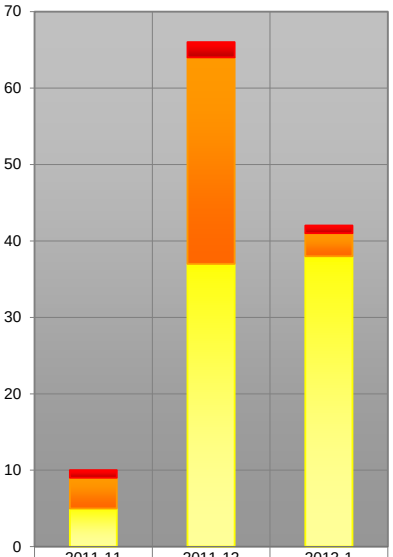
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an info-at-scip.ch. Gerne nehmen wir Ihre Vorschläge entgegen.

Auswertungsdatum:	19. Januar 2012



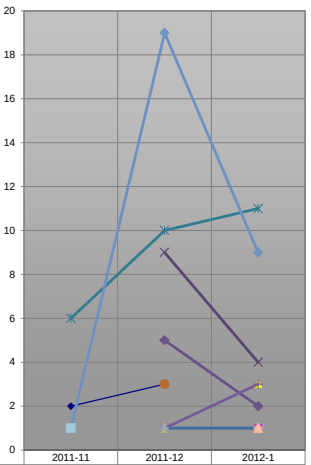
	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
sehr kritisch	56	15	15	6	11	11	21	10	8	1
kritisch	214	314	402	442	229	140	72	67	142	3
problematisch	170	287	423	396	419	176	70	81	124	38

Verlauf der Anzahl Schwachstellen pro Jahr



	2011-11	2011-12	2012-1
sehr kritisch	1	2	1
kritisch	4	27	3
problematisch	5	37	38

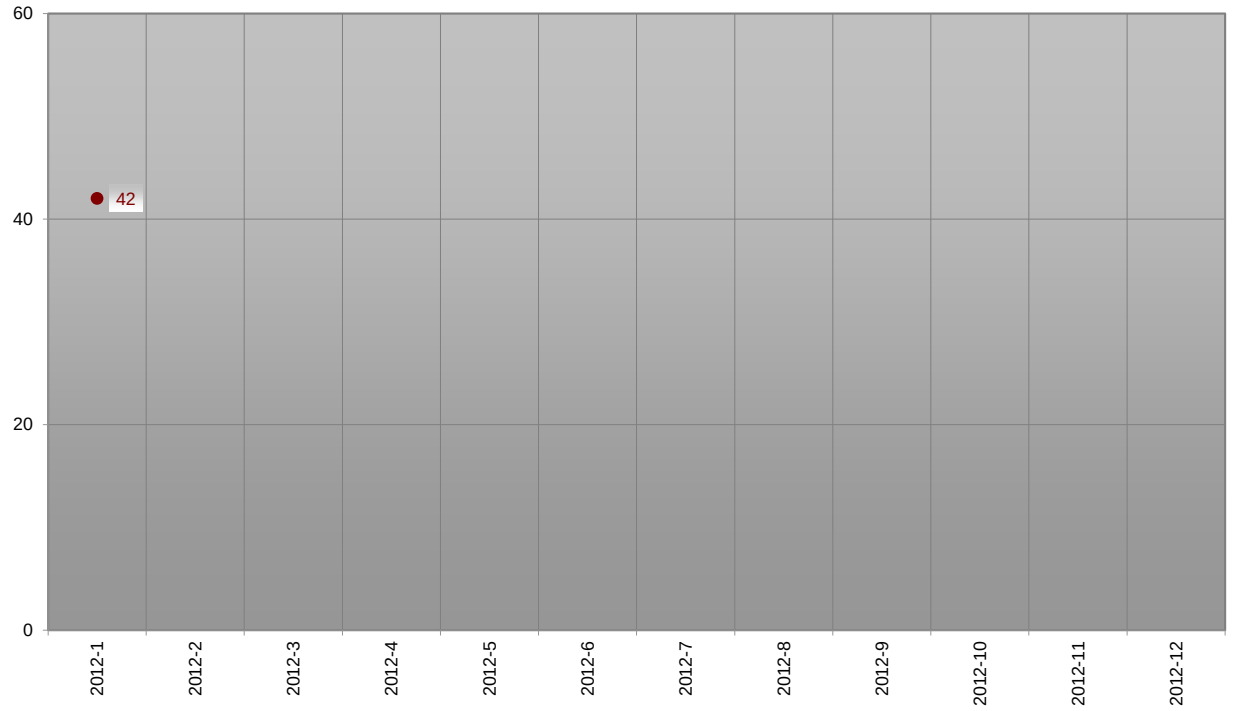
Verlauf der letzten drei Monate Schwachstelle/Schweregrad



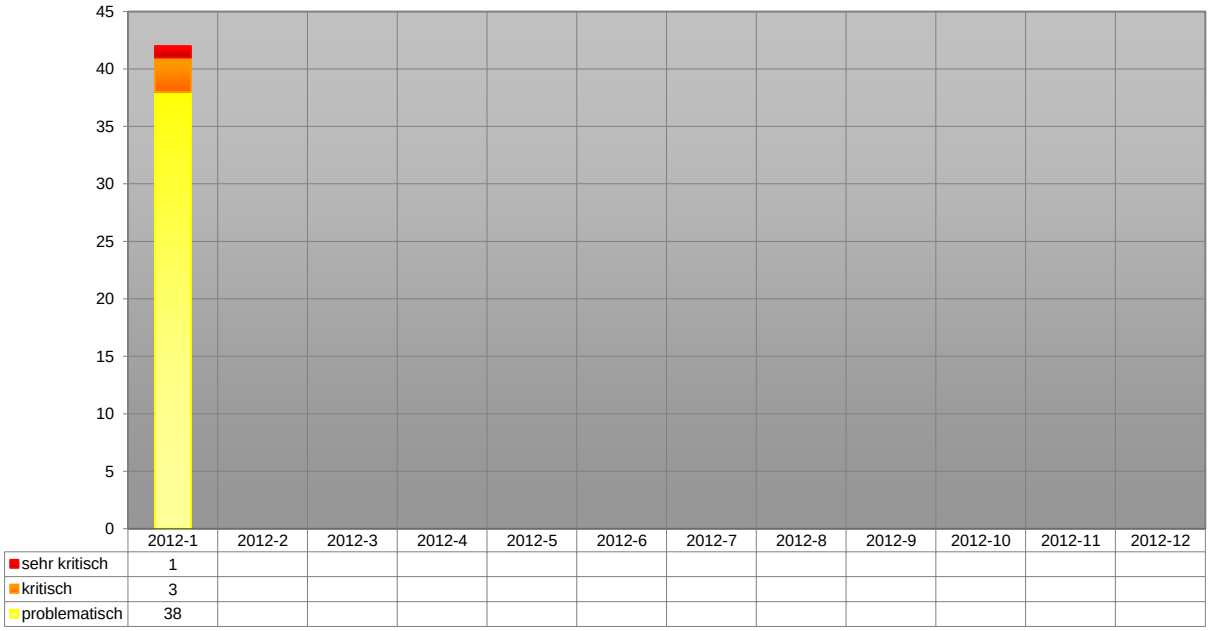
	2011-11	2011-12	2012-1
Unbekannt	2	3	
Code Injection			1
Command Injection			3
Cross Site Scripting		9	4
Denial of Service	6	10	11
Designfehler		3	
Directory Traversal		1	1
Eingabeungültigkeit			
erweiterte Rechte		5	
erweiterte Zugriffsrechte		5	2
Fehlende Authentifizierung			
Fehlende Verschlüsselung			
Fehlerhafte Leserechte			
Fehlerhafte Schreibrechte			
Format String			
Information Disclosure		1	3
Konfigurationsfehler			
Programmcode ausführen			1
Pufferüberlauf	1	19	9
Race-Condition			
Redirect		1	
Remote File Inclusion		1	
Schwache Authentifizierung			
Schwache Verschlüsselung			
Spoofing		1	
SQL-Injection			
Symlink-Schwachstelle			
Umgehungsangriff			1
Umgehungs-Angriff	1		
Umleitung			1

Verlauf der letzten drei Monate Schwachstelle/Kategorie

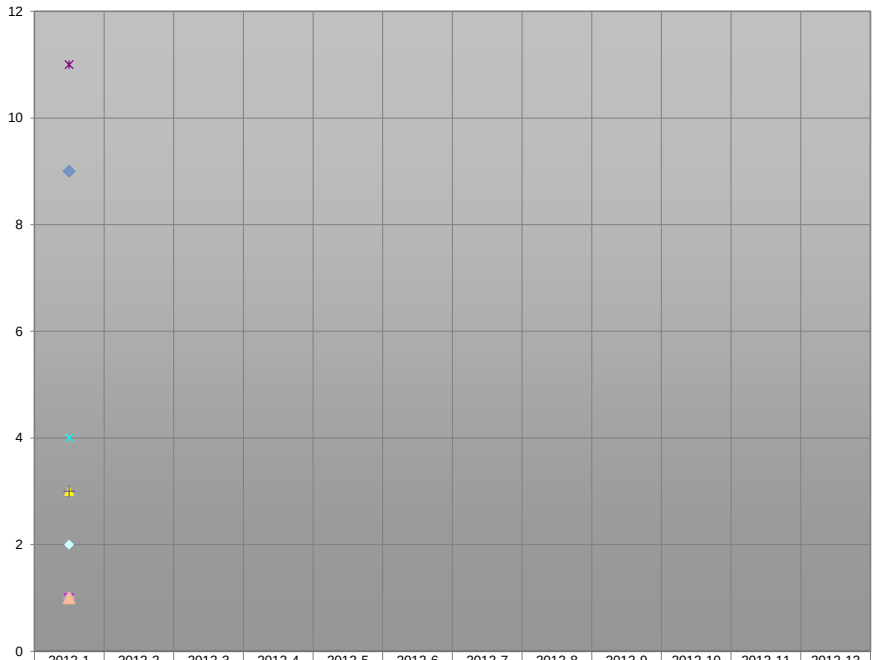
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2012



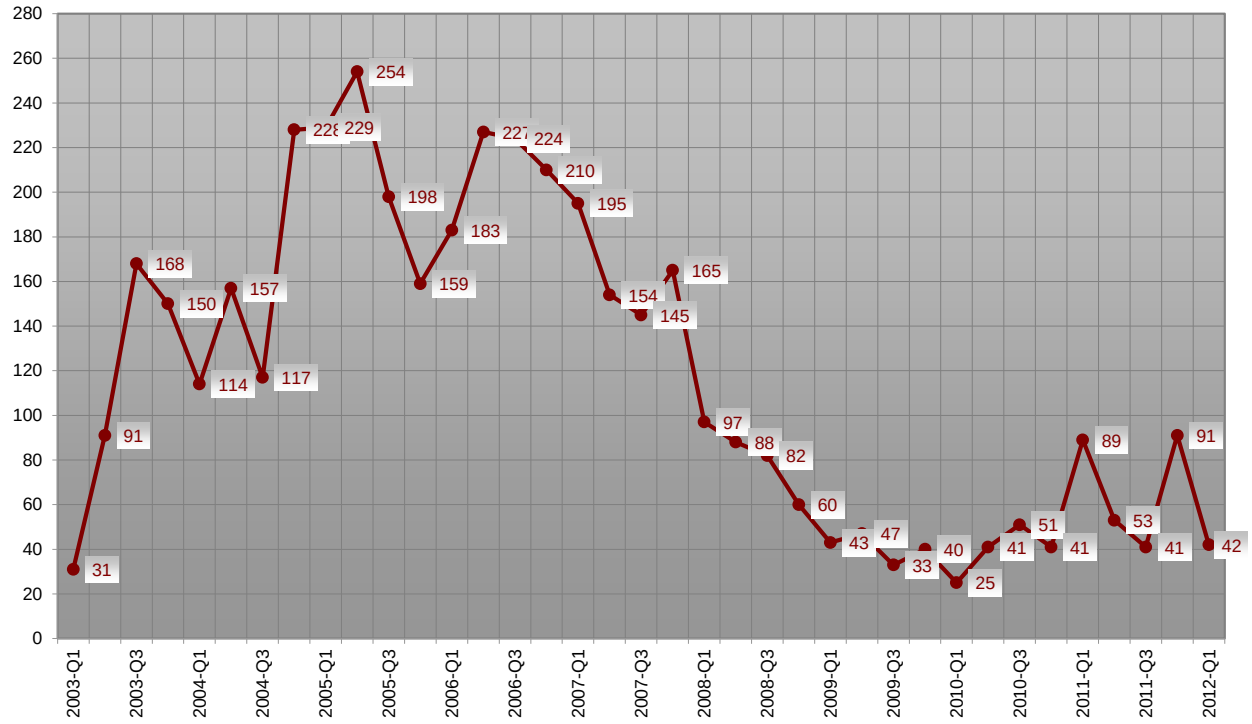
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2012



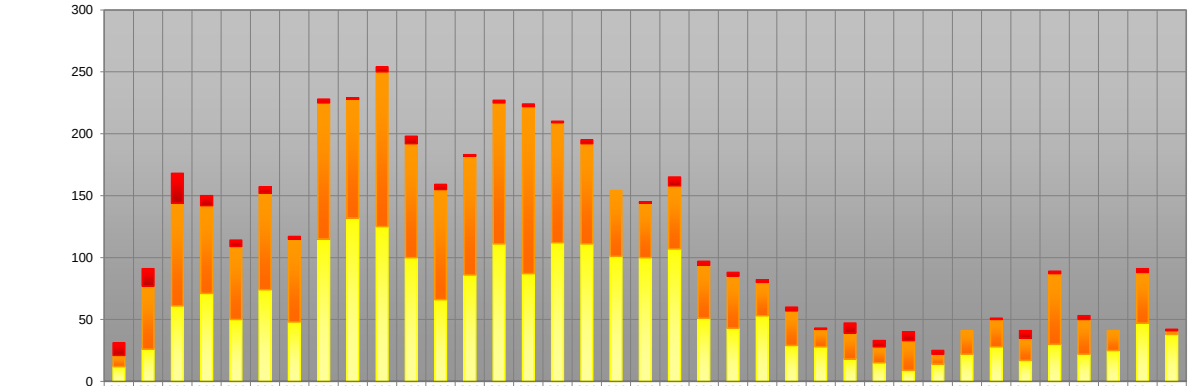
	2012-1	2012-2	2012-3	2012-4	2012-5	2012-6	2012-7	2012-8	2012-9	2012-10	2012-11	2012-12
Unbekannt												
Code Injection	1											
Command Injection	3											
Cross Site Scripting	4											
Denial of Service	11											
Designfehler												
Directory Traversal	1											
Eingabeungültigkeit												
erweiterte Rechte												
erweiterte Zugriffsrechte	2											
Fehlende Authentifizierung												
Fehlende Verschlüsselung												
Fehlerhafte Leserechte												
Fehlerhafte Schreibrechte												
Format String												
Information Disclosure	3											
Konfigurationsfehler												
Programmcode ausführen	1											
Pufferüberlauf	9											
Race-Condition												
Redirect												
Remote File Inclusion												
Schwache Authentifizierung												
Schwache Verschlüsselung												
Spoofing												
SQL-Injection												
Symlink-Schwachstelle												
Umgehungsangriff	1											
Umgehungs-Angriff												
Umleitung	1											

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2012

Registrierte Schwachstellen by scip AG

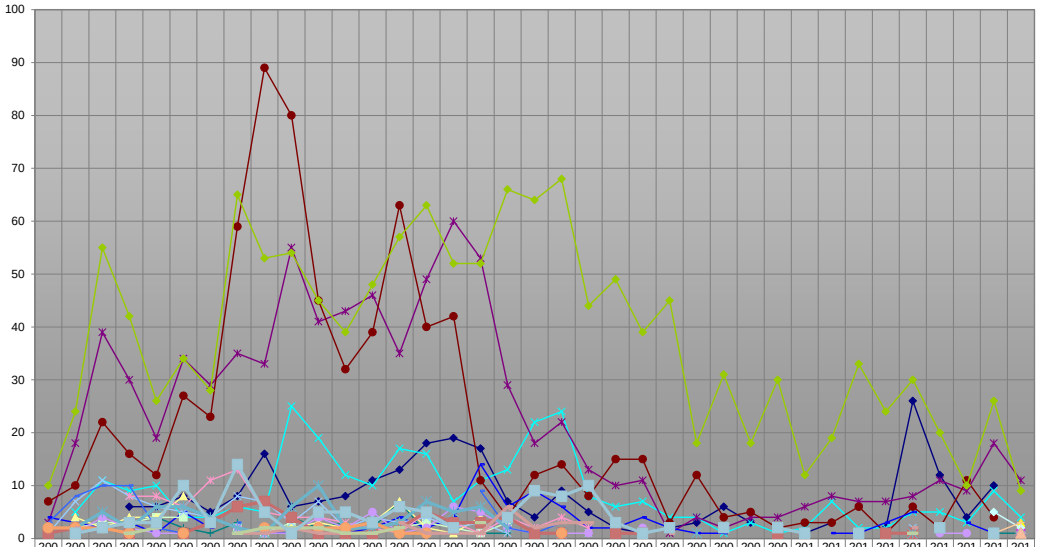


Verlauf der Anzahl Schwachstellen pro Quartal seit Q1/2003



	2003-Q1	2003-Q2	2003-Q3	2003-Q4	2004-Q1	2004-Q2	2004-Q3	2004-Q4	2005-Q1	2005-Q2	2005-Q3	2005-Q4	2006-Q1	2006-Q2	2006-Q3	2006-Q4	2007-Q1	2007-Q2	2007-Q3	2007-Q4	2008-Q1	2008-Q2	2008-Q3	2008-Q4	2009-Q1	2009-Q2	2009-Q3	2009-Q4	2010-Q1	2010-Q2	2010-Q3	2010-Q4	2011-Q1	2011-Q2	2011-Q3	2011-Q4	2012-Q1
sehr kritisch	10	14	24	8	5	5	2	3	1	4	6	4	1	2	2	1	3		1	7	3	3	2	3	1	8	5	7	3		1	6	2	3		3	1
kritisch	9	51	83	71	59	78	67	110	96	125	92	89	96	114	135	97	81	53	44	51	43	42	27	28	14	21	13	24	8	19	22	18	57	28	16	41	3
problematisch	12	26	61	71	50	74	48	115	132	125	100	66	86	111	87	112	111	101	100	107	51	43	53	29	28	18	15	9	14	22	28	17	30	22	25	47	38

Verlauf der Anzahl Schwachstellen/Schweregrad pro Quartal seit Q1/2003



	2003-Q1	2003-Q2	2003-Q3	2003-Q4	2004-Q1	2004-Q2	2004-Q3	2004-Q4	2005-Q1	2005-Q2	2005-Q3	2005-Q4	2006-Q1	2006-Q2	2006-Q3	2006-Q4	2007-Q1	2007-Q2	2007-Q3	2007-Q4	2008-Q1	2008-Q2	2008-Q3	2008-Q4	2009-Q1	2009-Q2	2009-Q3	2009-Q4	2010-Q1	2010-Q2	2010-Q3	2010-Q4	2011-Q1	2011-Q2	2011-Q3	2011-Q4	2012-Q1
Unbekannt				6	6	8	5	8	16	6	7	8	11	13	18	19	17	7	4	9	5	2	1	2	3	6	3		1	3		2	26	12	4	10	
Code Injection																																					1
Command Injection																																					3
Cross Site Scripting		5	11	9	10	4	4	6	5	25	19	12	10	17	16	7	11	13	22	24	8	6	7	4	4	1	3	1	2	7	2	2	5	5	3	9	4
Denial of Service	3	18	39	30	19	34	29	35	33	55	41	43	46	35	49	60	53	29	18	22	13	10	11	1	4	2	4	4	6	8	7	7	8	11	9	18	11
Designfehler	7	10	22	16	12	27	23	59	89	80	45	32	39	63	40	42	11	4	12	14	8	15	15	3	12	4	5	2	3	3	6	1	6	2	11	4	
Directory Traversal					4	2	1	3		4	2	3	2	7	1	1	1	1												1		1			1	1
Eingabeungültigkeit	4	3	2	3	1	5	2		1	1		1	2	4	2	4	14	6	9	6	2	2	4	2	1	1			1	1	3	5		3	1	
erweiterte Rechte																																			5	
erweiterte Zugriffsrechte																																			5	2
Fehlende Authentifizierung		2	3	3	4	4		2	1	3			1	2	3	2	1	3																		
Fehlende Verschlüsselung		4	2	4	4	8				2	3	2	3	7	2	1	4																			
Fehlerhafte Leserechte	1	7	11	8	6	5	4	8	7	3	7	2	4	3	4	2	3	1			1											2				
Fehlerhafte Schreibrechte				8	8	6	11	13	5	4	4	3	2	1	5	3	1	4	2	4	2											1				
Format String		1	4	2	1	1		2	1	1	4	2	5	1	2	6	5	2	1	1	1		2									1		1	1		
Information Disclosure																																			1	3
Konfigurationsfehler	3	8	10	10	2	1		3		1							9	2	1	3			1														
Programmcode ausführen																																				1
Pufferüberlauf	10	24	55	42	26	34	28	65	53	54	45	39	48	57	63	52	52	66	64	68	44	49	39	45	18	31	18	30	12	19	33	24	30	20	10	26	9
Race-Condition	1	2		1		1	3	6	7	4	1	1	1	2	5	3	3	4	1	1		1	1					1			1	1				
Redirect																																			1	
Remote File Inclusion																																			1	
Schwache Authentifizierung		2	5	2	6	6	4	2	1	6	10	2	2	3	7	5	6	2		1					1							1				
Schwache Verschlüsselung	2	2	2	1		1			2		2	2	3	1	1					1																
Spoofing																																			1	
SQL-Injection		2		1				1	1	2	1	1		3	1	1	1	6	2	3	3			1								2				
Symlink-Schwachstelle				1	2			1	2	2	2	1	1	2			3															1				
Umgehungsangriff																																				1
Umgehungs-Angriff		1	2	3	3	10	3	14	5	1	5	5	3	6	5	2		4	9	8	10	3	1	2		2		2	1		1			2		1	
Umleitung																																				1

Verlauf der Anzahl Schwachstellen/Kategorie pro Quartal seit Q1/2003

5. Labs

In unseren scip Labs werden unter http://www.scip.ch/?labs regelmässig Neuigkeiten und Forschungsberichte veröffentlicht.

5.1 Windows 8 Developer Preview Sicherheit

12.01.2012 Marc Ruef, maru-at-scip.ch

Microsoft stellt seit einigen Wochen die Developer Preview von Windows 8 zum Download zur Verfügung. Diese Pre-Beta kann durch Entwickler genutzt werden, um sich mit den neuen Gegebenheiten der nächsten Windows-Generation auseinanderzusetzen.

Wir haben mehrere Instanzen von Windows 8 in unserem Labor eingerichtet, um mittels funktionalen und sicherheitstechnischen Tests erste Rückschlüsse auf zukünftige Entwicklungen machen zu können. Unsere Erkenntnisse sollen in diesem Beitrag zusammengefasst werden.

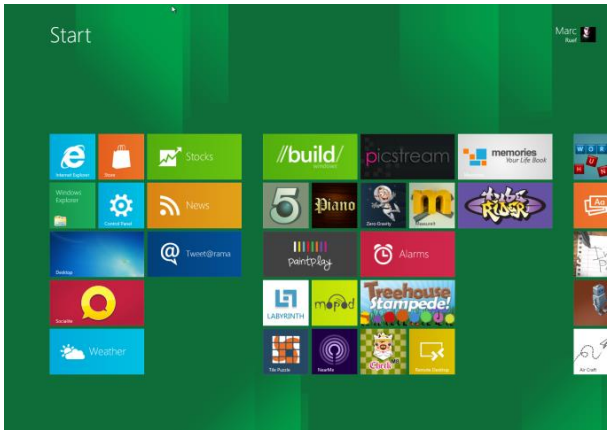
Installation
Die Installation war sehr effizient und einfach. In rund 20 Minuten liess sich ein System ohne grössere Komplikationen installieren. Dies war ebenfalls als virtuelle Instanz in VirtualBox möglich. Während der Installation lassen sich rudimentäre Einstellungen definieren. Zum Beispiel kann schon hier das Verhalten für das automatische Installieren von Patches bestimmt werden.

Die Standardeinstellungen entsprechen zu grossen Teilen jenen Definitionen, wie wir sie zu empfehlen pflegen. Vor allem Privatanwender werden grosse Vorteile durch die klaren Regelungen für sich gewinnen können. Unkompliziert lässt sich so ein funktionales und sicheres System aufbauen. Im professionellen Umfeld muss natürlich mit einem Mehr an Anpassungen gerechnet werden.

Login
Noch während der Installtion fragt Windows 8, ob die Installation an ein Live-Konto geknüpft werden soll. Entweder kann ein solches eingerichtet oder auf ein bestehendes zurückgegriffen werden. Die Registrierung erfolgt per Benutzername und Passwort. Dabei wird ein Email an das verknüpfte Mailkonto geschickt, in dem ein Aktivierungslink enthalten ist. Dadurch kann die Legitimität der Installation und des daran gebundenen Kontos bestätigt werden.

Das Einloggen mit dem Live-Konto ist interessant, da sich damit cloudähnliche Mechanismen realisieren lassen. Microsoft ist darum bemüht, dass Einstellungen systemübergreifend definiert und durch den entsprechenden Login synchronisiert werden können. Ein ähnliches Verhalten wird durch Mozilla Firefox mit den Sync-Optionen realisiert.

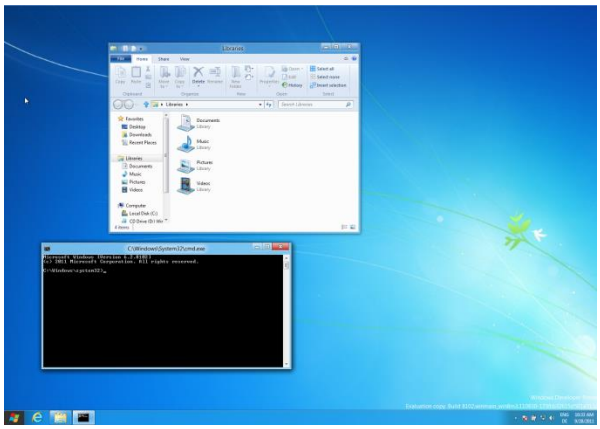
Neue Oberfläche
Das Credo beim grafischen Design von Windows 8 ist Simplizität. So kommen viele grafische Elemente mit sehr einfachen, oftmals rechteckigen Strukturen daher. Die neue Oberfläche namens Metro scheint dabei in erster Linie auf Tablets ausgerichtet zu sein. Relativ grosse Icons zeigen die einzelnen Anwendungen an, die durch einen Klick gestartet werden können. Diesen Stil hat Microsoft schon mit Windows Phone 7 auf ihren Mobiltelefonen eingeführt und bei der Xbox360 weitergenutzt.



Traditionelles System
Durch das Klicken auf das Icon Windows Explorer kann die klassische grafische Oberfläche geladen werden. Hier wird bestens bekannt die Taskleiste am unteren Rand des Bildschirms eingeblendet. Durch das Klicken auf den Windows-Button wird jedoch nicht mehr das Start-Menu geöffnet, sondern stattdessen wieder zum neuen GUI gewechselt. Programme, Dokumente und Einstellungen müssen neu aus dem Explorer heraus gestartet werden.

Einzig in einigen Bereichen haben Fenster ein kleines Redesign erhalten. So werden nun grössere Icons, wie man sie schon von Office 2010 her kennt, eingesetzt. Dies macht die Fenster auf den ersten Blick attraktiver und soll in erster Linie die MacOS X-Klientel ansprechen.

Durch Start/Ausführen können wie üblich Programme direkt angesteuert werden. Nach wie vor lässt sich damit die MS DOS-Eingabeaufforderung durch die Eingabe von cmd.exe starten. Sie begrüsst den Benutzer vorerst mit der Version 6.2.8102.



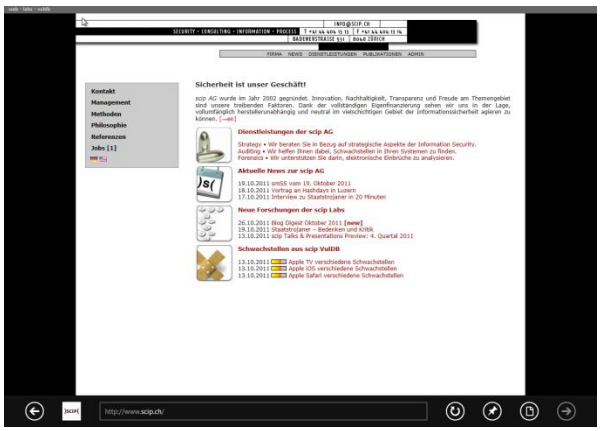
App Store
Ein bisschen abgeschaut von Apple, ist im Betriebssystem ein Store für den Download von Apps vorgesehen. In der ersten offiziellen Preview war dort lediglich ein Hinweis eingebracht, dass diese Funktion noch nicht freigegeben ist. Inwiefern sie sich verhalten wird, wird sich also zeigen.

Microsoft geht damit den Weg eines Walled Garden, der sicherheitstechnisch Vorteile mit sich bringen wird. Dadurch wird es möglich, Software auf Qualität und Sicherheit hin zu untersuchen, bevor eine offizielle Freigabe erteilt wird. Unsichere Produkte und Malware liessen sich so verhindern.

Dadurch fällt jedoch auf Seiten Microsoft ein Mehr an Aufwand an, was wiederum die Veröffentlichung von neuen und aktualisierten Produkten verzögert. Sicherheit wird diesem Fall zu Lasten von Offenheit und Flexibilität eingetauscht.

Internet Explorer
Als Standardbrowser kommt noch immer Microsoft Internet Explorer zum Tragen. Dieser hat in der Metro-Darstellung ein grundlegendes Re-Design erfahren und versucht sich an der Simplizität von Google Chrome anzuknüpfen. Die Menu-Elemente sind auf ein Minimum reduziert und so wird nur noch eine Adressleiste und Buttons für die wichtigsten Aktionen (z.B. zurück, neu laden) angezeigt. Während des Browsens werden gar auch diese Komponenten ausgeblendet, wodurch die Webseite in maximaler Grösse – schon fast Vollbild – dargestellt werden kann. Wem das nicht gefällt, der kann mit einem Mausklick in die klassische Ansicht wechseln.

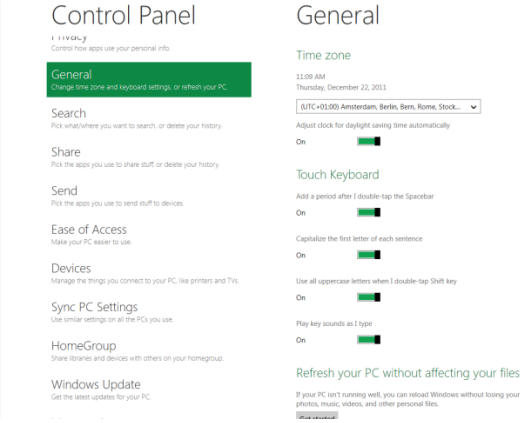
Leider kann man in der Preview das About des Browsers und damit die Version nicht ohne weiteres darstellen lassen. Als User-Agent gibt sich der neue Browser als Internet Explorer 10 aus. Ob es sich hierbei wirklich um die nächste Browser-Generation handelt, ist nicht sicher.



```
Mozilla/5.0 (compatible; MSIE 10.0;
Windows NT 6.2; Trident/6.0)
```

Die Einstellungsmöglichkeiten und das Verhalten bleiben damit eigentlich die gleichen, wie bei Internet Explorer 8 und 9. Hardening-Mechanismen, die schon bei Windows 7 zum Tragen gekommen sind, können entsprechend auch hier appliziert werden.

Sicherheitseinstellungen
Das Control Panel auf Metro kommt einmal mehr mit einer starken Vereinfachung daher. So werden nur die wichtigsten Einstellungsmöglichkeiten dargestellt, die sich jeweils mit einem Regler aktivieren oder deaktivieren lassen. Erst wenn auf More settings geklickt wird, wird die Systemsteuerung im klassischen Stil angezeigt. Sowohl die Darstellung als auch die Einstellungsmöglichkeiten orientieren sich an jenen von Windows 7.



Der detaillierte Vergleich der Auslieferung von Windows 7 und Windows 8 – in Bezug auf NTFS-Rechte und Registry-Einstellungen – fällt nahezu identisch aus. Nur in einigen wenigen Punkten sind Abweichungen festzustellen, die in vielen Fällen aber sowieso den individuellen Bedürfnissen der Umgebung angepasst werden müssen.

Fazit
Auf den ersten Blick wirkt Windows 8 wie eine komplett neue Windows-Generation. Dafür verantwortlich ist in erster Linie die Metro-Oberfläche. Lässt man die für mobile Geräte entwickelte Oberfläche aber ausser Acht und arbeitet mit dem klassischen Desktop, dann findet man sich in einer zu Windows 7 sehr ähnlichen Umgebung wieder.

Das Ziel von Windows 8 war sicherlich, die Einfachheit und Effizienz zu erhöhen, um mit iOS von Apple mithalten zu können. Ob dies gelungen ist, kann erst mit dem Einsatz auf entsprechenden Tablets bestätigt werden. Der erste Eindruck, wie zum Beispiel das Aufstarten des Systems, zeigen spürbare positive Verbesserungen.

Die ersten Sicherheitsmechanismen von Windows 8 sind aus Windows 7 übernommen und haben sich in den letzten Jahren bewahrheitet. Die Standardeinstellungen, die schon bei der Installation der neuen Windows-Generation angepasst werden können, versuchen eine Ausgewogenheit zwischen Sicherheit und Praktikabilität zu erreichen. Vor allem Privatanwender werden daraus einen Nutzen ziehen können. In professionellen Umgebungen, in denen zusätzliche Anforderungen an die Sicherheit gestellt werden, müssen zusätzliche Anpassungen angegangen werden.

6. Impressum

Herausgeber:
)SCIP(scip ag
scip AG
Badenerstrasse 551
CH-8048 Zürich
T +41 44 404 13 13
info-at-scip.ch
http://www.scip.ch

Zuständige Person:

Marc Ruef
Security Consultant
T +41 44 404 13 13
maru-at-scip.ch

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich Information Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserungen möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch. Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summarys finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. Anmelden! Abmelden!