[Chat zum CommunityCast]
Wie schütze ich mich vorm bösen Internet?
Microsofts Sicherheitstools im Einsatz

Kurzbeschreibung:

Leider gibt es eine Vielzahl von Möglichkeiten, wie sich unerwünschte Software auf dem Computer einnisten kann. In den meisten Fällen gelangt die Software über Internetseiten in das System, die so genannte Aktive Inhalte verwenden. Dabei handelt es sich um Skripte oder Programmteile, wie Java-Applets, JavaScript, VBScripte und ActiveX-Controls, deren Funktionen für den Besucher der Seite nicht sichtbar sind. Ursprünglich zur besseren Gestaltung gedacht, wird diese Funktion heute leider häufig missbraucht. Aber auch durch die Installation von eigentlich harmlos wirkender Free- und Shareware kann die unerwünschte Spyware in den Rechner gelangen. Die Programme selbst erfüllen zwar dabei ihren ursprünglichen Zweck, installieren aber heimlich Spionage-Funktionen mit. Selbst in kommerziellen Programmen können solche Spionage-Funktionen versteckt sein!

In diesem CommunityCast zeigen Michael Kalbe - Technologieberater für IT Sicherheit - und Kay Giza - Community Program Manager - wie man sich mit Software von Microsoft gegen diese Gefahren schützt. Das Zusammenspiel der Windows Firewall, Internet Explorers 7 und Windows Defender werden hierbei demonstriert.

CommunityCasts sind aufgezeichnete Videostreams, eine innovative Form von Online-Referaten, die direkt am Bildschirm verfolgt werden können.

Präsentiert von den Communities:
· www.winhilfe.ch
· www.protecus.de
· www.paules-pc-forum.de
· www.windows-tweaks.info
· www.giza-blog.de
· www.unterwegs-im.net

Download & Informationen: http://www.winhilfe.ch/wbb2/thread.php?threadid=21398

Transkript:

[19:05:16] **Shai Hulud**: Herzlich willkommen zu diesem Chat hier. Ich bedanke mich bei allen die gekommen sind (und noch kommen werden)
[19:05:34] **Shai Hulud**: Vielen Dank Michael und Kay dass ihr uns den Community-Cast zur Verfügung gestellt habt.
[19:05:45] Kay_(MSFT): Gerne immer wieder!
[19:05:46] **Shai Hulud**: Vielen Dank Dorothea für die gute Organisation des ganzen.
[19:06:05] Dorothea_MS: Hallo an alle! Als erstes möchte ich mich bei den Communities für die Unterstützung beim CommunityCast bedanken: http://www.winhilfe.ch, http://www.paules-pc-forum.de, http://www.windows-tweaks.info, http://www.protecus.de, http://www.giza-blog.de und http://www.unterwegs-im.net.
[19:06:20] Dorothea_MS: Dann natürlich auch vielen Dank an Wilfried Schmid von http://www.winhilfe.ch, dass er heute Gastgeber dieses Chats ist.
[19:06:22] **Shai Hulud**: wie ihr alle wisst gehts heute um Fragen zu dem Community-Cast "Wie schütze ich mich gegen das böse Internet"
[19:06:30] **Shai Hulud**: danke danke
[19:06:37] Dorothea_MS: Ein herzliches Dankeschön natürlich auch an Michael Kalbe und Kay Giza für den tollen CommunityCast und dafür, dass Ihr Euch heute Abend Zeit genommen habt, um an diesem Chat teilzunehmen.
[19:06:55] Dorothea_MS: Nun kurz zum Ablauf:
[19:07:08] Dorothea_MS: Michael und Kay werden nun all Eure Fragen beantworten. Aber bitte nicht durcheinander fragen, damit wir auch den Überblick behalten und auch wirklich alle Fragen

beantwortet werden.
[19:07:11] Tobbi verlässt den Chat.
[19:07:23] laquemanda: hallo kay
[19:07:26] Bastelmaus betritt den Raum.
[19:07:27] Dorothea_MS: Da Ihr bestimmt schon alle ganz gespannt seid und Eure Fragen loswerden wollt, übergebe ich hiermit an unsere beiden Experten.
[19:07:34] Dorothea_MS: Viel Spaß also beim Chat! Es kann losgehen!
[19:07:37] Kay_(MSFT): Hallo laquemanda.
[19:07:49] Kay_(MSFT): Hallo zusammen! Schön das ihr da seid!
[19:07:55] **Shai Hulud**: find ich auch
[19:08:08] **Shai Hulud**: traut sich keiner?
[19:08:11] Kay_(MSFT): Hat jemand von Euch eine Frage, ohne die er
[19:08:16] Michael_[MSFT]: und jetzt tauschen wir Kochrezepte aus, oder hat vielleicht jemand eine Frage? ;-)
[19:08:16] Kay_(MSFT): heute Nacht nicht schlafen könnte?
[19:08:19] Kay_(MSFT): Dann los....
[19:08:19] schotti111 betritt den Raum.
[19:08:35] Bastelmaus verlässt den Chat.
[19:08:38] Kay_(MSFT): Ansonsten würde ich mal in die Runde fragen wollen, wer von Euch Windows Devender gerade einsetzt....
[19:08:48] **Shai Hulud**: hier!
[19:08:48] Cat_UwiN: <-
[19:09:02] Michael_[MSFT]: Er meint natürlich Defender ;-)
[19:09:03] **Ste**: *hüstel*... nein
[19:09:10] Yusuf_Dikmenoglu: <-- setzt DEFENDER ein
[19:09:22] Lukas_(Protecus): <- ist neugierig geworden...
[19:09:29] Kay_(MSFT): ok ok - ich sagte ja... kann heute nicht schreiben. Wie ist Eure Erfahrung?
[19:09:32] gucky betritt den Raum.
[19:09:34] Dorothea_MS: Fenster V und Vogel F
[19:09:37] Dorothea_MS: :-)
[19:09:37] Yusuf_Dikmenoglu: <-- setzt Eigentlich alles von MSFT ein ;-)
[19:09:48] Lukas_(Protecus): mit f wie verkehrt
[19:09:52] Michael_[MSFT]: Auch Origami ?
[19:10:09] Kay_(MSFT): okaaaaaaay: Meinte Windows Defender....
[19:10:18] Yusuf_Dikmenoglu: Jajaa Micha, Du kommst natürlich mit Kanonen ;-)
[19:10:25] Darkman betritt den Raum.
[19:10:31] **Shai Hulud**: Für alle die später gekommen sind: Die Frage war: Wer setzt schon den MS Defender ein?
[19:11:02] Kay_(MSFT): Wie sind Eure Erfahrungen?
[19:11:13] Cat_UwiN: was mir gefaellt ist nach wie vor die geschwindigkeit vom defender
[19:11:28] Cat_UwiN: und dass meine maschine nicht komplett lahmgelegt ist
[19:11:45] Cat_UwiN: gefunden wurde leider bei mir noch nichts
[19:11:51] schotti111: Mit welcher Software ist Defender vergleichbar?
[19:11:56] Kay_(MSFT): Da kannst Du doch sehr froh sein.
[19:11:56] Cat_UwiN: meine kiste ist zu sauber
[19:12:01] **Shai Hulud**: stimmt wenn ich meinen Virenscanner starte dann kann ich mal eben alles andere abhaken
[19:12:02] Kay_(MSFT): Denn eine der häufigen Fragen die kommt, ist wie verhält sich das Programm mit anderen Softwareprodukten (AntiSpyware Produkten)
[19:12:08] Yusuf_Dikmenoglu: Was mir gefällt ist generell das es sowas gibt und das es "demnächst" im Betriebssystem integriert wird
[19:12:35] Kay_(MSFT): Ein Hinweis dazu von mir: Wenn ihr Windows Defender einsetzt, zusammen mit anderen Produkten, sollte normalerweise alles gut laufen.
[19:12:54] **Ste**: @Yusuf ist auch mehr als nötig, da die spyware Plage die Oberhand nimmt
[19:13:00] **Shai Hulud**: Der Defender ist am ehesten mit AdAware oder Spybot vergleichbar. Ein Programm dass Spyware anhand von Signaturen erkennt
[19:13:06] Akiramausi: also können alle anti vir programme weiterhin laufen?
[19:13:15] Cat_UwiN: akira, sollen sogar
[19:13:18] Kay_(MSFT): Es kann nur Hinweise geben, wenn ihr z.B. ein anderes Softwareprodukt einsetzt (und umgekehrt), welches Quarantäne-Verzeichnisse hat, dass hier dann Hinweismeldungen

kommen.
[19:13:30] Akiramausi: okay
[19:13:32] Yusuf_Dikmenoglu: @STE - Full ACK ;-)
[19:13:48] Cat_UwiN: der defender ergaenzt den schutz des rechners, er ersetzt niemals virenscanner, firewall und Das gehirn des users
[19:14:03] Kay_(MSFT): Akiramausi: also können alle anti vir programme weiterhin laufen? >> wie Cat sagt: Ja!
[19:14:24] **Shai Hulud**: Wenn Du ich sag mal Feierabend-PC-Supporter bist bei Privatpersonen: Bei fast jedem PC ist irgendwas drauf
[19:14:40] Cat_UwiN: shai, leider
[19:14:49] Darkman: Also ins Betriebsystem integrieren, damit waer ich etwas vorsichtig - optional wie jetzt ist ok - man sollte den user nicht zu sehr "entmuendigen" *find*
[19:14:58] **Ste**: schon jemand Erfahrung mit Errorsafe vs Windows Defender gemacht?
[19:15:01] Cat_UwiN: ich hoffe aber, dass sich das bewusstsein der nutzer in den naechsten jahren veraendert
[19:15:18] **Shai Hulud**: wir arbeiten alle miteinander dran
[19:15:30] Kay_(MSFT): @Ste: Nein - Du?
[19:15:39] Yusuf_Dikmenoglu: Aber wieviele Anwender nutzen noch nicht einmal einen Virenscanner :-(
[19:15:47] Kay_(MSFT): Erkläre doch mal kurz was das ist, Ste.
[19:15:54] Cat_UwiN: Yusuf, meine Mutter
[19:15:58] **Ste**: @Kay nein, daher die Frage, den zurzeit geht nur adaware
[19:16:00] Yusuf_Dikmenoglu:
[19:16:19] Cat_UwiN: da hab ich das teil eigenhaendig entsorgt .. bringt eh nicht viel, ohne internetzugriff
[19:16:30] **Ste**: @Kay Errorsafe?
[19:16:51] Yusuf_Dikmenoglu: Na dann, aber Du weißt ja, dann kommt die Tochter mit einem USB-Stick oder CD und schon kann es zu spät sein ;-)
[19:16:53] Schwabenpfeil! betritt den Raum.
[19:16:54] **Shai Hulud**: Ich frag mich bloss wie lange es dauert, bis die Spyware-Programmierer den Defender im Griff haben
[19:16:55] Kay_(MSFT): Jup - wir bieten ja auch ein Transkript an, den jeder nachlesen kann. So können wir anderen erklären, die dieses nicht wissen.
[19:17:20] **Shai Hulud**: ich will damit sagen: So manipulieren, dass er nichts mehr erkennt
[19:17:32] Cat_UwiN: shai, nennt sich rootkit
[19:17:37] Dorothea_MS: Hallo Schwabenpfeil!
[19:17:38] **Ste**: Also genauere Infos gibt es hier, arbeite seit längerem daran weil es eine grosse Plage ist http://www.winhilfe.info/Sicherheit/Saeuberung/ErrorSafe_20060129132/
[19:17:38] Lukas_(Protecus): stimmt und MS ist natürlich immer Angriffsziel No1
[19:18:01] Schwabenpfeil!: Hallo Dorothea! :-)
[19:18:05] **Ste**: Errorsafe nervt den User damit das sein Rechner infiziert ist so mit 500 - 1000 Bösartigen Programmen
[19:18:06] Michael_[MSFT]: @Shai, das wir mit Vista und UAC nahezu unmöglich
[19:18:14] Cat_UwiN: hiho schwabenpfeil
[19:18:25] Yusuf_Dikmenoglu: UAC in VISTA rockt ;-)
[19:18:42] Schwabenpfeil!: Hi!
[19:18:43] **Shai Hulud**: öhm was war noch gleich UAC ?
[19:18:47] **Ste**: man installiert es und um dann den rechner Sauber zu bekommen muss man zahlen, nebenbei wird noch alles Mögliche Installiert um den user auszuspionieren und mit Popups usw zu nerven
[19:19:06] Kay_(MSFT): @Shai und Michael: Außerdem gibt es eine große Community rund um Defender, die dafür sorgt, dass man immer auf dem aktuellen Stand ist.
[19:19:06] **Ste**: hallo Schwabenpfeil
[19:19:16] Michael_[MSFT]: User Accunt Control, sprich Du bist nicht als Admin unterwegs...
[19:19:24] **Shai Hulud**: hallo schwabenpfeil
[19:19:35] Cat_UwiN: Ste, das klingt ja erfreulich .. wo kann ich das laden?
[19:19:36] **Shai Hulud**: ooookay
[19:19:36] MaMü betritt den Raum.
[19:19:46] **Shai Hulud**: hallo mamü

[19:19:47] MaMü: Hallo
[19:19:52] Cat_UwiN: da hat sich einer richtig muehe gemacht
[19:19:54] Michael_[MSFT]: Dann schliesse ich mich an: Hallole schwobapfeil'le
[19:20:08] Kay_(MSFT): Hallo @ all die gerade dazu gekommen sind
[19:20:18] schotti111: wird bei vista der systembereich besser vor bösewichter geschützt?
[19:20:32] Cat_UwiN: schotti, ja
[19:20:42] Michael_[MSFT]: schotti, wie meinste denn das "besser"?
[19:20:45] Lukas_(Protecus): durch welche mittel?
[19:20:56] gucky: Läuft auf Vista durch TCPA eh nur noch das was vorher abgesegnet wurde?
[19:20:58] **Shai Hulud**: zumindest kannst der IE nicht mehr so einfach auf Daten ausserhalb seines Bereiches zugreifen
[19:21:13] Cat_UwiN: zb werden die services gehaertet ..
[19:21:17] Michael_[MSFT]: Also erst mal wurde ALLE systemdienste in Vista einem Hardening und Packaging unterzogen
[19:21:45] schotti111: Hallo Schwabenpfeil, zu spät gesehen...
[19:21:47] Michael_[MSFT]: sprich es wurde analysiert wozu der dienst benötigt wird und welche berechtigungen er "WO" braucht
[19:21:53] Michael_[MSFT]: und nur das kann er dann auch
[19:21:57] Yusuf_Dikmenoglu: Auch das in VISTA NAP (Network Access Protection) integriert ist, wird mit dem Longhorn Server das ganze noch sicherer
[19:22:53] **Ste**: neue Sicherheitsmassnahmen werden sicherlich neue art von Bedrohungen erzeugen, wie sieht es mit dem Nachrüsten von solchen "Unbekannten" aus?
[19:23:05] **Shai Hulud**: Akiramausi erzählt mir grad: Sie versteht nur bahnhof
[19:23:19] **Ste**: ist auch sehr technisch das ganze gerade....
[19:23:37] **Shai Hulud**: und ich hab das Gefühl wir müssen uns auf das Level des Casts herunterbewegen
[19:23:51] Akiramausi: nein, bitte nicht wegen mir
[19:23:52] Kay_(MSFT): Akiramausi: Hast Du eine spezielle Frage? Rufe einfach laut, wenn Du was nicht verstehst.
[19:24:03] Akiramausi: ich weiß ja wer es mir dann noch einmal haarklein erklärt ;-)
[19:24:19] Kay_(MSFT): Doch genau wegen Dir und allen anderen machen wir ja den Chat.
[19:24:27] Yusuf_Dikmenoglu: Yepp
[19:24:29] Cat_UwiN: akiramausi, ich stelle mich freiwillig zur verfuegung
[19:24:41] Kay_(MSFT): Wenn Du einen guten Einstiegspunkt zum Thema Windows Vista haben möchtest, dann schaue dir mal die Seite http://www.windowsvista.de an.
[19:24:43] **Shai Hulud**: ich seh mich schon wieder tage am telefon hängen ....
[19:24:51] Akiramausi: also in erster linie vewirren mich die vielen abkürzungen
[19:25:04] Akiramausi: okay, danke kay ;-)
[19:25:08] Kay_(MSFT): Dann rufe laut - und wir erklären Dir die Abkürzungen - ok?
[19:25:21] **Ste**: @Kay da steht als im Vista Blog
[19:25:40] Michael_[MSFT]: ich seh keine Abkürzung, welche z.B.
[19:25:43] **Ste**: ich meinte mehr
[19:25:45] Kay_(MSFT): Außerdem haben Michael und ich in unseren Blogs einige weitere hilfreiche Links gepostet, die Du dir anschauen kannst.
[19:25:49] Dorothea_MS: Frage von Ste bitte nicht vergessen: neue Sicherheitsmassnahmen werden sicherlich neue art von Bedrohungen erzeugen, wie sieht es mit dem Nachrüsten von solchen "Unbekannten" aus?
[19:26:28] Cat_UwiN: TCPA = Trusted Computing Platform Alliance
[19:26:37] Cat_UwiN: @ akira mausi
[19:26:48] Akiramausi: dankeschön ;-)
[19:26:53] Kay_(MSFT): Ste - wie meinst Du das genau? Wie man sich vor neuen Bedrohungen schützen kann?
[19:26:54] Darkman: tcpa is boese.. [tm]
[19:27:00] Michael_[MSFT]: TCPA gibts nimmer, dafür heisst es jetzt TPM Trusted plattform module
[19:27:02] Cat_UwiN: und das ist eine ziemlich hart umstrittene geschichte
[19:27:12] **Shai Hulud**: allerdings
[19:27:23] Michael_[MSFT]: das ist ein eigener speicherbereich in welchem schlüssel aufbewahrt werden
[19:27:24] Cat_UwiN: michael, jep .. aber ist immernoch dasselbe
[19:27:33] Cat_UwiN: und die abkuerzung fiel oben
[19:27:50] Darkman: Kay: ich glaub er moechte wissen ob es moeglichkeiten gibt sich von neuen

sachen im "vorraus", also praeventief, zu schuetzen bzw. wie schnell es moeglich ist, auf neue Bedrohungen zu reagieren
[19:27:56] Michael_[MSFT]: ist nichts neues, kennen viele schon von der Smartcard (siehe Deine EC karte oder Krankenkassenkarte)
[19:28:20] Darkman: aeh, naja, also TPM und ne EC Karte sollte man vlt. dann doch nicht vergleichen 
[19:28:25] Michael_[MSFT]: er meint also Microsoft Glasskugel V1.09a ?
[19:28:42] nhr-av team betritt den Raum.
[19:28:44] Kay_(MSFT): OK. Grundsätzlich (um die generische Frage zu beantworten) ist die gesamte Architecture von Windows Vista darauf ausgelegt, genau gegen solche Unbekannten zu reagieren und zu agieren.
[19:28:49] Tobbi betritt den Raum.
[19:28:53] Tobbi: .
[19:28:59] Michael_[MSFT]: Natürlich kann man das vergleichen, der Speicherbereich ist derselbe (vom aufbau)
[19:29:09] Darkman: nein, keine Glaskugel, siehe das was der IE7 auf Vista mitbringt, das "Sandbox" Feature - sowas koennte man ja "generell" haben fuer alles.. das wuerde zumindest die huerde hoeher legen und ist praeventief
[19:29:46] Michael_[MSFT]: und nennt sich UAC und ist Bestandteil von Vista
[19:29:54] Kay_(MSFT): Zusammen mit anderen Produkten (wie im Cast beschrieben) und der Möglichkeit von Updates, ist man natürlich gegen "Unbekannte" grundsätzlich geschützt. Eine 100% Sicherheit kann niemand gerantieren (das geht nicht).
[19:30:17] Michael_[MSFT]: Damit liegt die Hürde schon recht hoch
[19:30:22] Kay_(MSFT): Aber Ste, wie oben beschrieben, gibt es
[19:31:36] **Ste**: sorry war kurz rüben um die anderen her zu holen, muss kurz nachlesen...
[19:31:36] Tobbi verlässt den Chat.
[19:31:45] Kay_(MSFT): diverse Software (wie IE7) und diverse, ich sage mal grundsätzliche Hürden (wie Benutzerkontoschutz (User Account Control)), um Unbekannten gut zu begegnen.
[19:32:04] nhr-av team verlässt den Chat.
[19:32:08] Tobbi betritt den Raum.
[19:32:27] Tobbi verlässt den Chat.
[19:32:35] gucky: Hilft das UAC nur im Bezug auf den IE7 oder auch bei normalen exploidversuchen?
[19:33:01] dominikberger betritt den Raum.
[19:33:21] Kay_(MSFT): @Gucky:
[19:33:24] Darkman: Michael: UAC ist aber nix anderes als "als user arbeiten" (was man ja immer sollte, trotzdem keiner tut usw.) - das IE Sandboxing geht weiter, es gibt einen "Bereich" vor in dem sich der IE "bewegen" darf (halt nicht einfach irgendwo auf die platte schreiben etc. - auch nicht wenns der user eigentlich duerfte!) - sowas generell fuer (bestimmte?) Applikationen (vorallem solche die eben Anfaellgi sind fuer Angriffe aus dem Netz) waer doch gleich noch viel besser
[19:33:25] Akiramausi: was ist ein exploidversuch?
[19:33:56] Kay_(MSFT): unter Windows XP steht dieser wegen der anderen Konzeption des Betriebssystems nicht zur Verfügung (beim IE7) --> ?Protected Mode?.
[19:34:04] Darkman: Akiramausi: Exploitversuch -> Der Versuch eine Schwachstelle in einem Programm auszunutzen um Schadcode o.ae. auszufuehren
[19:34:07] **Shai Hulud**: ein exploid ist ein PRogramm was gezielt ein Sicherheitsloch ausnutzt
[19:34:24] Tobbi betritt den Raum.
[19:34:31] Akiramausi: danke euch beiden ;-)
[19:34:38] Kay_(MSFT): @ Gucky: Grundsätzlich gestattet dieses bei Windows Vista dem Internet Explorer 7 nicht, Dateien außerhalb des Ordners mit temporären Internetdateien zu verändern, sodass der Webbrowser quasi in einer isolierten Umgebung läuft.
[19:34:58] Michael_[MSFT]: @Darkman: richtig, deswegen kannst Du ja auch Virtalisierung dafür verwenden. Das für jede Applikation zu verwenden ist eine sehr aufwändige implementierung
[19:34:59] Yusuf_Dikmenoglu: @Michael - lässt sich DEFENDER in VISTA wenn der Longhorn Server draußen ist, zentral verwalten ?
[19:35:09] Michael_[MSFT]: vielleicht sehen wir das in Zukunft mal ;-)
[19:35:35] **Shai Hulud**: Virtualisierung? ich frage für die die sich nicht trauen
[19:35:45] Michael_[MSFT]: @Yusuf: sagen wr es mal so, wir denken darüber nach ;-)
[19:35:56] Darkman: Michael: ja klar, alles immer in einzelne Umgebungen packen is "too much" - aber grade Anwendungen wie IE, Outlook, MediaPlayer, Messenger etc. koennte man per default reinpacken...
[19:36:36] Yusuf_Dikmenoglu: @Shai - Virtualisierung, möchtest Du erklärt haben was das genau

bedeutet?
[19:37:06] Michael_[MSFT]: @Darkman: und dann wären da noch diverse VoIP Applikationen und Webservices die ich dort sehen würde. Du siehst meinen Punkt, eigentlich bist Du immer online..
[19:37:15] Darkman: Shai/Wer sich nicht traut: Virtualisierung beschreibt den Prozess eine Applikation in eine eigene, virtuelle und isolierte Umgebung zu packen. Stells Dir quasi vor als "Rechner im Rechner" (wobei der Rechner im Rechner nur das noetigste kann/koennen sollte das die Applikation laeuft). Damit "sichert" man diese Applikation ab bzw. den eigenen Rechner vor der Applikation da sie keinen vollen Zugriff mehr auf das System haben kann
[19:37:24] **Shai Hulud**: nee ich nicht, aber ich kann mir schon denken wer
[19:37:24] Kay_(MSFT): @Ste: Gucky: Frage beantwortet ?
[19:37:49] Cat_UwiN: Shai, Virtualisierung ist das zur Verfuegung stellen von Diensten, die einen in sihc abgeschlossenen Raum zur verfuegung haben, eine "virtuelle" umgebeng
[19:37:51] **Ste**: @kay ja
[19:38:01] **Shai Hulud**: ich habs verstanden
[19:38:17] gucky: hm ich glaube schon
[19:38:26] Darkman: Michael: klar, aber fangen wir "klein" an. Bei MS eigener Software hat MS die Chance dies durchzuziehen und, ganz ehrlich, die genannten Applikationen sind mit die Hauptangriffsziele - also waer damit doch zumindest den vielen Endusern schonmal viel geholfen..
[19:38:57] **Shai Hulud**: ich finde das ist ein Riesenschritt in die richtige Richtung
[19:39:33] Yusuf_Dikmenoglu: @Shai - ich finde seit Windows 2000 geht es schon in die richtige Richtung
[19:39:34] Darkman: Shai: es ist definitiv ein Schritt in die richtige Richtung - riesig waer er gewesen, wenn mans wirklich durchgezogen haette.. ;-)
[19:39:36] **Ste**: ich denke das es ein Problem löst und die spyware einen anderen Weg finden werden, der Kampf ist also unendlich, nichts tun wäre aber auch Falsch
[19:39:38] Michael_[MSFT]: Richtig, daher auch die Implementierung des IE7, Outlook 2007 wird einen Ähnlichen Mechanismus bereitstellen...
[19:39:46] Kay_(MSFT): Grundsätzlich Gucky: Wenn Du administrative Sachen ausführen möchten, wie z. B. Programminstallationen, wird Vista dich fragen, willst Du es wirklich, und dies bevor Du oder das Programm administrative "Dinge" ausführen können. Auf diese Weise wird die Verwendung von Administratorberechtigungen minimiert, wodurch es für bösartige Software (Malware) wie Viren, Würmer, Spyware und andere potenziell unerwünschte Programme schwieriger wird, den PC weitreichend zu befallen.
[19:40:27] **Ste**: Aber der normale user drückt doch einfach so auf OK ohne nachzudenken oder zu wissen was er da macht...
[19:40:30] gucky: ok, genau das wollte ich wissen
[19:40:44] Darkman: Hat sich jemand eigentlich mal mit dem theoretischen Angriff befasst, das auf Vista ein Programm laeuft, das diese "Popups" verdeckt/automatisch beantwortet? Sowas wird z.B. heute schon eingesetzt um unsignierte Treiber zu installieren (leider)
[19:40:53] Michael_[MSFT]: @Darkman, wirklich durchgezogen, verstehe ich in diesem Kontext nicht. Alle genannten Applikationen lassen sich so konfigurieren das dein risko kalkulierbar bleit
[19:41:03] Yusuf_Dikmenoglu: @Ste - nicht nur die Anwender, da gibt es auch viele Admins die das einfach so machen ;-9
[19:41:07] Cat_UwiN: Ste, das ist das Problem .. alle technik nutzt nichts, wenn der User nicht seinen Verstand einsetzt
[19:41:27] Darkman: Michael: "lassen sich so" <- nicht "durchgezogen" vs. "wird per default wie der IE mit diesem Sandboxing ausgeliefert" <- durchgezogen
[19:41:33] Michael_[MSFT]: In Vista wir es nicht möglich sein unsignierte Treiber zu installieren....
[19:41:49] Cat_UwiN: Michael, in allen versionen?
[19:41:50] **Ste**: @Cat_UwiN meistens ist es einfach nur die unwisenheit, bzw wenn das Programm so tut als ob es gut wäre denkt der unerfahrende Media Markt käufer das auch
[19:42:03] Cat_UwiN: Ste *nick*
[19:42:05] Kay_(MSFT): Apropos , @all: Kennt ihr den Spruch: Phishers Phritze phisht phrische Phische?
[19:42:09] **Shai Hulud**: Ja der neueste Trend ist es ja, Schadsoftware als Treiber zu installieren
[19:42:09] Robs betritt den Raum.
[19:42:12] Yusuf_Dikmenoglu: @Michael - GAR NICHT mehr - unsignierte Treiber ? N da werden sich einige Hersteller umschauen müssen ... aber nur gut für die Anwender
[19:42:16] Michael_[MSFT]: ? Alle Applikationen nutzen die Virtuellen verzeichnisse, Sandboxing ist der Falsche begriff

[19:42:22] Cat_UwiN: kay, den hab ich schon geblogt
[19:42:32] Sandro_Villinger betritt den Raum.
[19:42:36] Yusuf_Dikmenoglu: @Kay - Mmmuuhhhhhhhaaaaaaaaaaaaaaaaaa
[19:42:37] Michael_[MSFT]: IE7 läuft im "protected mode" also im USERCONTEXT
[19:42:38] Cat_UwiN: hi sandro
[19:42:40] **Shai Hulud**: hallo Sondro!
[19:42:41] **Ste**: Sandbox kannte ich nur aus Google Sprache....
[19:42:50] **Ste**: Hallo Sandro
[19:42:50] Robs verlässt den Chat.
[19:42:50] Sandro_Villinger: Hi! Konnte nicht früher :-)
[19:42:52] Kay_(MSFT): Ohh - dann habe ich das überlesen... ich wollte Euch nur auf einen sehr guten Artikel hinweisen: http://www.codezone.de/DetailPage.Codezone?GUID=4fe7b247-735d-47ff-8610-67a934c0872b
[19:42:52] **Shai Hulud**: ups Sandro
[19:43:07] Michael_[MSFT]: es gilt also für ALLE APPLIKATIONEN auf Vista, nix Autostart, Registry etc. änderbar!
[19:43:26] Kay_(MSFT): Eine lesenswerte Einführung ins Thema „Phishing“ und „Pharming“.
[19:43:42] Michael_[MSFT]: Also wenn Du das meinst haben wir es durchgezogen und zwar komplett!
[19:43:43] Dorothea_MS: @ Sandro: Schön, dass Du es geschafft hast!
[19:44:17] **Shai Hulud**: Das ist ja wie im Western!
[19:44:23] Kay_(MSFT): Mal kurz eine Pause in die Runde um zu fragen: Gab noch offene Fragen die eventuell untger gegangen sind?
[19:44:26] **Shai Hulud**: Der Revolverheld betritt die Szene
[19:44:33] **Shai Hulud**: ggg
[19:44:47] **Shai Hulud**: War nur Spass Sandro
[19:44:50] Yusuf_Dikmenoglu: @Michael - GAR NICHT mehr - unsignierte Treiber ? Na da werden sich einige Hersteller umschauen müssen ... aber nur gut für die Anwender
[19:45:15] Darkman: Michael: also kann unter Vista ein frisches Outlook (dem was mit Vista kommt/was dann verfuegbar ist) nicht ohne weiteres in den Autostartordner schreiben ("Bug" im Outlook vorrausgesetzt der das ermoeglicht) und das ohne das der User was tun muss (ausser eben die mail zu lesen o.ae.)?
[19:45:32] Michael_[MSFT]: @Yusuf: GAR NICHT, genau hast Du das Echo in den Medien etwa nicht mit bekommen?
[19:45:41] Sandro_Villinger: Ach du hattest es von mir???
[19:46:01] Sandro_Villinger: Ich bin doch kein Revolverheld - at least, nicht immer
[19:46:11] Michael_[MSFT]: @Darkman: Jetzt sind wir beieinader: Genau DAS geht mit Vista nimmer
[19:46:45] gucky: Und wenn ich bei mir Avast (Vierenscanner installiere und der sich eintragen möchte?
[19:47:46] Kay_(MSFT): @Gucky: Mache das jetzt mal mit laufendem Windows Defender, dann wirst Du merken, dass Du gefragt werden wirst (Möchtest du das? Ja/Nein)
[19:48:00] Yusuf_Dikmenoglu: @Kay - Du kennst das Remote Programm Dameware ? Das meckert bei mir der Defender permanent an :-(
[19:48:28] Michael_[MSFT]: @Yusuf: dann solltest Du ein Ausnahme definieren ;-)
[19:49:03] Kay_(MSFT): Ok - das habe ich auch bei ein zwei Programmen. Dafür kann man dann der "Community" beitreten und so helfen, die Software (derzeit in der Beta-Phase) zu verbessern.
[19:49:39] Yusuf_Dikmenoglu: ei des tun wir doch ;-)
[19:50:34] **Shai Hulud**: Ich hab noch eine Frage wegen der Phishing-Funktion
[19:50:47] Kay_(MSFT): Her damit!
[19:51:02] Kay_(MSFT):
[19:51:03] **Shai Hulud**: Wie wird dann schlussendlich entschieden welche Seite Phishing oder sonstwie böses enthält?
[19:51:10] **Shai Hulud**: ich meine, nach Anzahl?
[19:51:29] Kay_(MSFT): Du meinst beim IE7, hmm was meinst Du mit Anzahl?
[19:51:33] **Ste**: ja und wie kommt es das die Adsense Seite als bösartig eingestuft wird?
[19:51:36] **Shai Hulud**: ich hab ne tolle Seite aber die Konkurrenz trommelt genug leute zusammen um mich schlecht zu machen?
[19:51:57] Kay_(MSFT): Nein - mom - einer nach dem anderen und eine Frage beantworten nach der anderen...
[19:52:30] Michael_[MSFT]: hallo
[19:52:45] Kay_(MSFT): Grundsätzlich: Beim Aufruf einer Webseite wird die Website-URL, die der

Anwender besucht, mit einer Liste bekannter Phishing-Website vergleichen.
[19:53:15] Kay_(MSFT): Handelt es sich um eine verdächtige oder tatsächliche Phishing-Website, zeigt das der Internet Explorer 7 in seiner - dann gelb bzw. rot unterlegten - Sicherheitsstatusleiste rechts neben der Adressleiste unmissverständlich an. Da Aktualität beim Anti-Phishing besonders wichtig ist, nimmt Microsoft eine regelmäßige Aktualisierung der Liste bekannter Phishing-Websites vor. Zusätzlich können Anwender die gerade angesteuerte Website als Verdachtsfall per Mausklick melden.
[19:53:40] Kay_(MSFT): Das haben wir ja im CommunityCast gezeigt.
[19:53:41] **Shai Hulud**: so und da ist doch die Falle
[19:53:59] **Shai Hulud**: also meine Konkurrenz klickt fleissig auf Denunzierung
[19:54:18] Michael_[MSFT]: Nein, das ist nicht möglich
[19:54:18] Kay_(MSFT): D.h. es wird überprüft(!) werden und ist kein automatischer(!) Mechanismus.
[19:54:28] **Shai Hulud**: und ich als armer einzelner Seitenbetreiber kann nur sagen stimmt doch gar nicht
[19:54:38] Michael_[MSFT]: genau das kannst du machen
[19:54:55] Kay_(MSFT): Du hast ja auch als Betreiber einer Webseite (wie im Cast erwähnt), die Möglichkeit, dich zu äußern.
[19:55:05] Darkman: wie oft soll die Liste eigentlich aktualisiert werden?
[19:55:16] Michael_[MSFT]: welche Liste?
[19:55:19] gucky: Wieviele personelle kapatzitäten wird Microsoft dafür verwenden? Ich meine, wn der IE7 genauso oder verbreiteter wie der IE6 wird gibs sicher ne Menge Meldungen...
[19:55:22] Yusuf_Dikmenoglu verlässt den Chat.
[19:55:25] Darkman: die Phishingseitenliste
[19:55:48] Kay_(MSFT): Es gibt da keinen fest definierten Zeitraum. Wenn es nötig ist bzw. "on the fly". Genaues kann ich Dir dazu nicht sagen. Michael?
[19:55:48] Michael_[MSFT]: Ok hier scheint ein Missverständnis vor zu liegen
[19:55:53] Yusuf_Dikmenoglu betritt den Raum.
[19:55:55] Akiramausi: also versteh ich das richtig? die dort gemeldeten websites werden kontrolliert, und wenn sie doch ich sage mal clean sind, kommen sie nicht in diese liste?
[19:55:56] **Ste**: Info am Rande, ich bin weg >> Abendessen ruft, ich lasse den Chat an um in ruhe alles nachzulesen
[19:56:07] Michael_[MSFT]: der IE Phishingfilter lässt sich in 3 Stufen unterteilen
[19:56:11] **Shai Hulud**: tschüüü ste
[19:56:14] Cat_UwiN: ste, mahlzeit
[19:56:20] Yusuf_Dikmenoglu: @Ste - Buon Appetit
[19:56:31] Tobbi verlässt den Chat.
[19:56:32] Akiramausi: guten hunger ste ;-)
[19:56:36] **Ste**: Grazie mille
[19:56:45] Michael_[MSFT]: 1. IE7 kennt ~85.000 well know also Gute Seiten per se
[19:56:54] Gast betritt den Raum.
[19:57:07] Dorothea_MS: Vielen Dank an Ste!
[19:57:09] Yusuf_Dikmenoglu: 85.000 bei 100000000000000 Webseiten ;-)
[19:57:24] Gast verlässt den Chat.
[19:57:36] Kay_(MSFT): Yusuf - lass uns doch mal den Michael schreiben
[19:57:38] Michael_[MSFT]: 2. IE7 erkennt phishing sites selbst (hierzu werden über 1000 checks durchgeführt beim aufruf eine seite)
[19:58:16] Kay_(MSFT): Beispielsweise wird die zu besuchende URL-Adresse überprüft, ob diese ungewöhnliche Zeichen enthält bzw. eine ungültige Syntax aufweist und dadurch eine ganz andere Webseite als die eigentlich Gewünschte referenziert.
[19:58:20] Michael_[MSFT]: 3. IE7 nutzt die an einen zentralen Server gemeldeten und durch einen manuellen Prozess überprüften sites
[19:58:36] Michael_[MSFT]: damit "weiss" ie ob gut oder böse
[19:58:48] Michael_[MSFT]: mal gaaanz simpel erklärt
[19:59:00] **Shai Hulud**: aaach deshalb ist Winhilfe auf die Liste gerutscht, wegen der Weiterleitung!
[19:59:08] Dorothea_MS: @all: Sind eigentlich von oben noch Fragen offen?
[19:59:27] **Shai Hulud**: ste hatte da was ich such
[19:59:36] Dorothea_MS: Nicht, dass wir jemanden übergangen haben?
[19:59:47] **Shai Hulud**: Ste: ja und wie kommt es das die Adsense Seite als bösartig eingestuft wird?
[19:59:51] Darkman: soviel ist mir auch klar, mir geht es nur darum wie "aktuell" die auf dem Zentralen Server gelagerte Liste mit "boesen" Seiten ist.. sprich, wie lang dauert es ca.(!) von der Meldung einer Seite (durch viele?) bis zum Eintrag in diese Liste

[19:59:54] Michael_[MSFT]: vermutlich, kann auch an der syntax liegen. steuerst du z.b. http://ip.ip.ip.ip an, dan schlägt IE7 an
[19:59:55] **Shai Hulud**: ich denke das ist geklärt
[20:00:02] **Shai Hulud**: Ste: ja und wie kommt es das die Adsense Seite als bösartig eingestuft wird?
[20:00:16] Kay_(MSFT): Wie im CommunityCast gezeigt, kann das u.U. auch bei einer Webseite passieren, die nicht Umleitet etc. - es unterliegt halt dem von Michael erklärten Weg (denn man dann korrigieren kann - wenn falsch)
[20:00:50] Michael_[MSFT]: je mehr eine seite gemeldet wird desto schneller ist sie entsprechend als böse markiert. ziel ist es in jedem fall eine kurze zeit zu erreichen
[20:01:03] Darkman: (Gibts ne Mail an den Betreiber oder so? ala "Herzlichen Glueckwunsch, Sie sind jetzt auf der Liste"?
[20:01:20] Yusuf_Dikmenoglu: Right - alla Blacklist
[20:01:24] **Shai Hulud**: du merkst es ja selber
[20:01:33] **Shai Hulud**: wenn du den ie7 benutzt
[20:01:38] Kay_(MSFT): Nein Darkman: Umgekehrt kannst Du dich aber melden.
[20:01:41] Cat_UwiN: shai, nicht alle benutzen den IE7
[20:01:44] Michael_[MSFT]: eine mail gibts nicht
[20:01:45] Typografix betritt den Raum.
[20:01:56] Darkman: Shai: woran? ich bin kein IE User und bin viel Unterwegs - ausserdem surf ich doch nicht staendig auf meine eigene Seite - ich weiss doch was da steht!
[20:02:00] Akiramausi: hallo thomas
[20:02:03] Tobbi betritt den Raum.
[20:02:06] **Shai Hulud**: stimmt. aber zumindest der Webseitenbetreiber wird wohl dazu gewzungen
[20:02:21] Kay_(MSFT): Wozu wird wer gezwungen?
[20:02:28] Michael_[MSFT]: na vielleicht wenn deine Anwender sich bei dir beschweren?
[20:03:01] gucky: Außerdem muss man ja nur am Anfang, solange dieser Schutz neu ist, gucken das die eigene Seite richtig erkannt wird
[20:03:11] Typografix: nabend @ all
[20:03:16] gucky: hi
[20:03:17] Darkman: ich faends nett wenn man schon gelistet wird, das dann zumindest an den Netzbetreiber/Domainbesitzer (laesst sich ja schnell rausfinden, wunderbar zur automatisierung!) ne Nachricht rausgeht... immerhin kanns ja auch sein das man kompromitiert wurde o.ae...
[20:03:29] MaMü: Hi Typo
[20:03:30] Michael_[MSFT]: Ich denke nicht das Ihr mit euren sites unter das raster fallt
[20:04:03] Kay_(MSFT): Es ist doch etwas grundsätzliches was hier geschieht, über das man froh sein kann. Wie in dem o.g. Phishing-Artikel beschrieben, gibt es sehr viele dieser Arten. Wenn Du einen Hinweis bekommst, den Du definitiv korrigieren möchtest, dann machst Du dieses. Oder?
[20:04:04] Michael_[MSFT]: @Darkman: wer sagt dir das dort immer der richtige ansprechpartner steht
[20:04:22] Cat_UwiN: an der stelle kann ich nur sagen, es gibt komische Sites auf dieser Welt, und manche davon besuche ich vielleicht auch absichtlich
[20:04:43] Kay_(MSFT): Cat: Dann kannst Du dieses ja auch gerne machen
[20:04:48] Michael_[MSFT]: wenn ich daran denke was es für ein akt war meine adresse bei den providern ändern zu lassen... glaube ich nicht das auch nur annäherd die infos dort stimmen bzw. verwertbar sind
[20:04:53] Sandro_Villinger: Vielleicht Trivialwissen, doch es sei an der Stelle vielleicht interessant...
[20:04:54] Darkman: Michael: zumindest wenns um den Netzbetreiber geht ists eigentlich mehr als unwahrscheinlich das die Infos falsch sind - die werden ja an verschiedenen Stellen verwendet
[20:05:21] Sandro_Villinger: Der Phishing-Check im IE7 wird asynchron zur Datenübertragung genutzt d.h. auch bei mehr als 5 Tabs verlängern sich die Ladezeiten nicht
[20:05:30] Michael_[MSFT]: ja und dann, dann weiss dein netzbetreiber das deine seite gelistet ist, UND?
[20:05:47] Sandro_Villinger: ich hatte da vorletzte woche auf der mix06 zeit, mit dem ie-team zu quatschen und da wurde das versichert
[20:05:56] Lukas_(Protecus) verlässt den Chat.
[20:06:33] Yusuf_Dikmenoglu: @Sandro - Interessant ;-) - was gab es noch alles auf der mix06 ?
[20:06:59] Tobbi: findest Du doch auf http://www.windows-tweaks.info
[20:07:14] Dorothea_MS: @all: Entschuldigt, wenn ich etwas unsanft unterbreche. Michael steht Euch nur noch für ein paar wenige Minuten zur Verfügung. Habt Ihr noch spezielle Fragen an Michael?

[20:07:19] Sandro_Villinger: @ Yusuf: Das war eine der Top-Fragen ans IE-Team, wenns um Phishing ging - daher
[20:07:23] Kay_(MSFT): Nur noch Mal kurz: Ist der Modus gut erklärt worden vom Filter?
[20:07:57] Darkman: Michael: ich betreibe selber Netze, wenn bei uns Mails eingehen das bestimmte IPs "auffaellig" sind, informieren wir den Kunden bzw. nehmen z.B. auch die Seiten vom Netz - das hilft dann auch leuten die keinen IE7 nutzen
[20:08:48] Michael_[MSFT]: Na prima!
[20:09:13] Dorothea_MS: Letzte Frage an Michael?
[20:09:19] Michael_[MSFT]: Wenn sich das ganze etabliert hat, denke ich wird es sicherlich für Netzbetreiber möglichkeiten geben
[20:09:42] laquemanda: adieu an alle und danke
[20:09:50] **Shai Hulud**: bitte bitte
[20:10:08] Kay_(MSFT): *winks* @ laquemanda
[20:10:14] Dorothea_MS: Kay wird noch etwas länger für Fragen zur Verfügung stehen...
[20:10:21] **Shai Hulud**: Keiner mehr eine Frage?
[20:10:23] Michael_[MSFT]: OK, an dieser Stelle möchte ich mich verabschieden
[20:10:30] Cat_UwiN: hey, aber ich haette noch eine kleine anmerkung
[20:10:33] **Shai Hulud**: Vielen vielen Dank Michael!
[20:10:35] Akiramausi: dankeschön michael
[20:10:38] Michael_[MSFT]: mein kleiner Sohn (6,5 Wochen) wartet schon auf mich
[20:10:39] Kay_(MSFT): ciao Michael!
[20:10:39] Cat_UwiN: der comcast war echt gut
[20:10:44] Cat_UwiN: vielen dank!
[20:10:45] Yusuf_Dikmenoglu: Huhuu Michael - GOOD JOB ;-)
[20:10:47] MaMü: Cu Michael
[20:10:48] Michael_[MSFT]: bleibt mir nur noch mals danke zu sagen
[20:10:49] Dorothea_MS: Vielen Dank an Michael, dass Du Dir die Zeit genommen hast!
[20:10:53] Michael_[MSFT]: für die vielen Fragen
[20:11:01] Michael_[MSFT]: ich hoffe ich konnte einiges klären
[20:11:02] **Shai Hulud**: ciao michael
[20:11:06] laquemanda verlässt den Chat.
[20:11:11] Michael_[MSFT]: solltet Ihr noch weitere fragen haben
[20:11:16] **Oropax** betritt den Raum.
[20:11:19] Michael_[MSFT]: wendet euch gerne an:
[20:11:20] **Shai Hulud**: wir reden bestimmt noch öfter nich?
[20:11:24] Cat_UwiN: klar .. wir kennen deine email
[20:11:37] Michael_[MSFT]: http://blogs.technet.com/mkalbe/contact.aspx
[20:11:38] Yusuf_Dikmenoglu: wir wissen wo Du wohnst
[20:11:46] **Shai Hulud**: ich leite das notfalls weiter
[20:12:05] Dorothea_MS: Danke auch an Deinen kleinen Sohn und Deine Frau, dass sie Dich so lange mit uns geteilt haben!!!
[20:12:19] Yusuf_Dikmenoglu: Yepp
[20:12:20] Michael_[MSFT]: Nicht vergessen, immer schön auf meine Blog schauen im April gibt es viele Neuigkeiten zu vermelden *grins*
[20:12:21] Kay_(MSFT): *winks* Michael!
[20:12:32] Cat_UwiN: *winks*
[20:12:43] Michael_[MSFT]: Also bis dann ciao ciao....
[20:12:45] Dorothea_MS: Ciao, Michael!
[20:12:47] **Shai Hulud**: ciao
[20:12:48] Sandro_Villinger: Tschüss Michael!
[20:12:59] Akiramausi: ciao
[20:12:59] Michael_[MSFT]: und wech.....isser
[20:13:04] Yusuf_Dikmenoglu: Cy@@ Micha
[20:13:04] Dorothea_MS: Kay steht wie gesagt noch weiter zur Verfügung.
[20:13:10] Michael_[MSFT] verlässt den Chat.
[20:13:19] Kay_(MSFT): So - noch mal zurück zu kommen... war das soweit erklärt mit dem Phishing-Filter?
[20:13:37] Yusuf_Dikmenoglu: <-- sagt JA
[20:13:54] Kay_(MSFT): Gut!

[20:13:59] Kay_(MSFT):
[20:14:00] Lukas_(Protecus) betritt den Raum.
[20:14:54] Dorothea_MS: Also: Fragen an Kay?
[20:14:55] Kay_(MSFT): Habt ihr noch fragen? Wie z.B. wie entfernt Defender denn Sachen? Worauf müsste man achten?
[20:14:57] **Shai Hulud**: wie siehts aus, hat noch einer was auf dem herzen??
[20:15:04] Yusuf_Dikmenoglu: @Kay - wann erscheint die Final vom Defender, weiß man das schon ?
[20:15:05] Dorothea_MS: Haben wir die Fragen oben geklärt?
[20:15:16] Tobbi: cu
[20:15:23] **Shai Hulud**: cu Tobbi
[20:15:26] Tobbi verlässt den Chat.
[20:15:30] Kay_(MSFT): cu Tobbi!
[20:15:33] Dorothea_MS: Bye Tobbi
[20:15:52] Dorothea_MS: Frage von Yusuf_Dikmenoglu: @Kay - wann erscheint die Final vom Defender, weiß man das schon ?
[20:15:58] nhr-av team betritt den Raum.
[20:16:11] Yusuf_Dikmenoglu: Danke
[20:16:38] **Shai Hulud**: ist so ein Spywareentferner wirklich einmal Final?
[20:16:40] Kay_(MSFT): Das ist eine gute Frage, ich weiß es gerade aus dem Kopf nicht. Ich denke es wird sich ähnlich wie Windows Vista verhalten. Ich kann das fix nachschlagen wenn Du möchtest.
[20:16:42] Yusuf_Dikmenoglu: Jetzzt iss er umgefallen
[20:16:58] gucky: bye
[20:17:02] Yusuf_Dikmenoglu: Nein, reicht schon - THX
[20:17:09] gucky verlässt den Raum.
[20:17:41] Yusuf_Dikmenoglu: Wird es in VISTA nun integriert sein, oder als zusätzliches Programm ?
[20:17:43] **Shai Hulud**: Der Cast war so gut, da bleiben kaum Fragen offen
[20:17:46] Kay_(MSFT): OK - ich werde das noch mal in meinen Blog aufgreifen und dem Post http://www.giza-blog.de/CommunityCastWieSchuetzeIchMichVormBoesenInternetMicrosoftsSicherheitstools ImEinsatz.aspx hinzufügen.
[20:17:57] **Shai Hulud**: Was mich etwas gestört hat ist die Tonqualität am Anfang
[20:18:06] Kay_(MSFT): Ja - es wird nahtlos integriert sein.
[20:18:06] **Oropax** verlässt den Chat.
[20:18:07] MaMü: In wie fern wird die Windows Firewall unter Vista erweitert? Einstellmöglichkeiten?
[20:18:25] Kay_(MSFT): @Shai: Wir werden uns bessern
[20:19:09] **Shai Hulud**: Die wichtigste Neuerung ist, dass die Firewall nicht nur von aussen nach innen, sondern auch von innen nach aussen wirkt
[20:19:10] Akiramausi: hey shai, sie habennur ab und an den kopf weggedreht und etwas getrunken ;-)
[20:19:17] Akiramausi: das sollte gestattet sein ;-)
[20:19:56] Kay_(MSFT): Genau Akiramausi
[20:20:39] nhr-av team: Inwieweit kann Windows Defender heute schon mit Rootkits umgehen, erkennen, entfernen?
[20:20:40] Akiramausi: besser als das ständige knacken: mico an, micro aus ;-)
[20:20:55] **Shai Hulud**: Kay kannste noch was zu Guckys Frage sagen?
[20:20:59] Kay_(MSFT): @Gucky... Du warst es mit der Firewall, gell?
[20:21:24] Schwabenpfeil!: OK, ich muss dann leider auch wieder weg. Danke an CLIP und winhilfe.ch für den Cast und den Chat! Man sieht sich! Ciao!
[20:21:25] Dorothea_MS: Nein MaMü
[20:21:36] MaMü: ich wars
[20:21:37] Dorothea_MS: Gucky ist nicht mehr da....
[20:21:53] Dorothea_MS: Ciao Schwabenpfeil!
[20:22:02] **Shai Hulud**: oops sorry mamü
[20:22:04] Kay_(MSFT): Also um so ein paar Schlagworte (sorry - meinte MaMü) zu sagen: Sie unterstützt eingehenden und ausgehenden Netzwerkverkehr.
[20:22:12] Kay_(MSFT): Ausnahmen können jetzt für Active Directory-Konten und -Gruppen, für Quell- und Ziel-IP-Adressen, für IP-Protokollnummern, für Quell- und Ziel-TCP- und UDP-Ports, für alle oder bestimmte TCP- und UDP-Ports, für bestimmte Schnittstellen, für bestimmte Dienste und für ICMP- und ICMPv6-Netzwerkverkehr konfiguriert werden.

[20:22:54] Kay_(MSFT): Ein (neues) Snap-In für die Microsoft Management Console (MMC) wurde integriert...
[20:22:58] Yusuf_Dikmenoglu: @KAy - und auch hier die Frage, lässt sich die FW auch Zertral verwalten (was ich schwer hoffe) ?
[20:23:13] MaMü: also bräuchte man theoretisch keine Drittanbieter firewall mehr? sprich norton, bitdefender?
[20:23:22] **Shai Hulud**: ja ich glaub das geht über Gruppenrichtlinien
[20:23:32] Schwabenpfeil! verlässt den Chat.
[20:23:43] Kay_(MSFT): Die brauchst Du heute auch nicht. Genau wie die aktuelle Windows Firewall in Windows XP Service Pack 2 (SP2) und Windows Server 2003 Service Pack 1 (SP1) handelt es sich auch bei der Windows Firewall um eine Host-Firewall, mit der Netzwerkverkehr blockiert werden kann. Anwendungen sind so vor böswilligen Benutzern und Programmen im Netzwerk geschützt.
[20:23:58] Yusuf_Dikmenoglu: @Mamü - Deine genannten FW brauchst Du ab XP-SP2 schon nicht mehr ;-)
[20:24:41] **Shai Hulud**: Duhuu Key, da haste in Deinem Satz wieder pfundweise Abkürzungen reingeworfen
[20:24:48] **Shai Hulud**: äh Kay
[20:24:49] Lukas_(Protecus): ich denke schon... die windows firewall ist ja nicht wirklich application based...
[20:24:54] Lukas_(Protecus): zumindest versucht das nur
[20:25:19] Kay_(MSFT): Mom: Yusuf_Dikmenoglu: Wie meinen? @Shai: Welche meinst Du? Warte ich erkläre...
[20:25:25] Yusuf_Dikmenoglu: Ist ja schließlich auch eine Software Firewall
[20:25:27] Lukas_(Protecus): siehe hier: http://www.firewallleaktester.com/tests.php
[20:26:13] Kay_(MSFT): Welche Abkürzungen meinst Du denn?
[20:26:18] **Shai Hulud**: ICMP, ICMPV6, TCP UDP
[20:26:42] **Shai Hulud**: Aber wir können einen rundumschlag machen
[20:26:58] Yusuf_Dikmenoglu: @Kay - na wenn ich an 500 Clients einen Port/Anwendung freischalten will, dass ich das quasi mit "einem-Klcik" erledigen kann (Stichwort: über GPO)
[20:27:17] Akiramausi: Ausnahmen können jetzt für Active Directory-Konten und -Gruppen, für Quell- und Ziel-IP-Adressen, für IP-Protokollnummern, für Quell- und Ziel-TCP- und UDP-Ports, für alle oder bestimmte TCP- und UDP-Ports, für bestimmte Schnittstellen, für bestimmte Dienste und für ICMP- und ICMPv6-Netzwerkverkehr konfiguriert werden.
[20:27:23] Cat_UwiN: ICPM = Internet Control Message Protokoll
[20:27:38] Akiramausi: um das zu verstehn, muss ich glaube ich eine ganze weile herumsuchen ;-)
[20:27:52] Cat_UwiN: das ganze nochmal fuer das neue Format, v6 (laenger besser, komplizierter)
[20:27:56] Yusuf_Dikmenoglu: @CAT - ICMP ;-)
[20:28:07] Akiramausi: bitte steinigt mich nicht gleich, das video war wirklich suuuper verständlich.
[20:28:13] Kay_(MSFT): Danke für die Begriffserklärungen.
[20:28:26] Akiramausi: aber dieser chat verwirrt mich einfach sehr :-(
[20:28:32] Yusuf_Dikmenoglu: TCP = Transmission Control Protocol
[20:29:22] Yusuf_Dikmenoglu: UDP = User Datagramm Protocol - http://de.wikipedia.org/wiki/UDP
[20:29:32] Kay_(MSFT): @Yusuf: Grundlegend kannst Du es hier nachlesen:
http://www.microsoft.com/technet/community/columns/cableguy/cg0106.mspx
[20:30:53] Kay_(MSFT): Nach oben liest und schaut ob eine Frage übersehen habe...
[20:31:57] Yusuf_Dikmenoglu: @Akiramausi - Ich empfehle Dir die Abkürzungen die hier genannt wurden, alle bei WIKIPEDIA nachzulesen, dort sind sie sehr gut erklärt ;-)
http://de.wikipedia.org/wiki/Hauptseite
[20:32:06] Kay_(MSFT): Hmm - also wenn keine Fragen mehr sind - dann würde ich mich gerne verabschieden wollen?
[20:32:17] Yusuf_Dikmenoglu: Ack
[20:32:23] **Shai Hulud**: ok
[20:32:38] Lukas_(Protecus): vielen Dank!!!
[20:32:48] Akiramausi: danke yusuf, ich versuch das mal
[20:32:49] Cat_UwiN: danke kax
[20:32:51] Cat_UwiN:
[20:32:55] Cat_UwiN: und guten heimweg
[20:32:56] Akiramausi: danke kay ;-)
[20:33:00] Sandro_Villinger verlässt den Chat.
[20:33:02] Yusuf_Dikmenoglu: Vielen Dank an MICROSOFT und WINHILFE und ganz besonders an

Dorothea für das managen und Kay für das beantworten
[20:33:06] **Shai Hulud**: danke Dir Kay
[20:33:17] **Shai Hulud**: Schön dass Du mitgemacht hast
[20:33:19] Kay_(MSFT): OK, ich lese das Transkript noch Mal durch und offene Fragen beantworte ich gerne unter http://www.giza-blog.de/CommunityCastWieSchuetzeIchMichVormBoesenInternetMicrosoftsSicherheitstools ImEinsatz.aspx oder bei Michael im Blog.
[20:33:36] **Shai Hulud**: Ich möchte mich zum Schluss nochmal bei allen für die Teilnahme am Chat bedanken.
[20:33:46] Dorothea_MS: Vielen Dank an Kay!
[20:33:52] Yusuf_Dikmenoglu: @Shai - und wir bei Dir - hat Spaß gemacht ;-)
[20:33:57] Dorothea_MS: Fürs lange durchhalten!
[20:34:02] nhr-av team: Thanks off and out
[20:34:02] Kay_(MSFT): Gerne - es hat sau Spaß gemacht!
[20:34:07] **Shai Hulud**: Besonderen DANK gilt natürlich auch Microsoft für die Bereitstellung des CommunityCasts
[20:34:07] Dorothea_MS: Und den tollen CommunityCast!
[20:34:16] Lukas_(Protecus): ich fand das für den Anfang schon sehr gut - war stark mal so ein CommunityCast kennenzulernen!
[20:34:16] nhr-av team verlässt den Chat.
[20:34:18] Cat_UwiN: dem kann ich mich nur anschliessen
[20:34:20] Kay_(MSFT): Danke an Euch für die vielen Fragen, wovon wir hoffentlich einige beantorten konnten.
[20:34:24] Dorothea_MS: Auch nochmals Danke an unsere Gastgeber von http://www.winhilfe.ch - wir würden uns freuen, Euch bei einem der nächsten CommunityCasts wieder begrüßen zu dürfen!
[20:34:38] Yusuf_Dikmenoglu: DDAAAAAAAAANNNNNNNNNNNNKKKKKKKKKKKKEEEEEEEEEEEEEEEEEEEEEEEEEEEE
[20:34:42] dominikberger verlässt den Chat.
[20:34:51] **Shai Hulud**: Bitte sehr! Machen wir doch gerne! Wir sind ja jetzt geübt
[20:34:58] Dorothea_MS: Vielen Dank für Eure vielen Fragen und Eure Teilnahme!
[20:35:16] Yusuf_Dikmenoglu: Nächstes mal sehen wir uns bei http://www.unterwegs-im.net ;-)
[20:35:17] Kay_(MSFT): Dann sage ich mal "Vielen Dank", bis die Tage! Ich verabschiede mich in 4 Wochen Urlaub
[20:35:31] Cat_UwiN: Du .... (den rest schenke ich mir)
[20:35:33] Yusuf_Dikmenoglu: und ich in 10 Tagen
[20:35:35] Cat_UwiN: viel spass kay
[20:35:37] Dorothea_MS: Viel Spaß im Urlaub!
[20:35:43] MaMü: Danke Kay und Viel Spass
[20:35:46] Kay_(MSFT): Danke! Und noch mal - war super!
[20:35:48] Kay_(MSFT): ciao!
[20:35:50] Akiramausi: oh, viel spaß und immr gutes wetter ;-)
[20:35:54] Yusuf_Dikmenoglu: Cy@@@ Kay
[20:36:05] Kay_(MSFT): <-- ciao und weg isser
[20:36:07] **Shai Hulud**: Was an Fragen noch kommen sollte, einfach an mich. ich leite das weitert. Ihr könnt natürlich auch im Forum fragen
[20:36:11] Lukas_(Protecus): vielen Dank an das MS&Winhilfe Team!
[20:36:11] Kay_(MSFT) verlässt den Chat.
[20:36:13] Lukas_(Protecus): ciao
[20:36:22] **Shai Hulud**: ciao Kay
[20:36:29] Typografix: mal den Leuten von MFST danke sage, auch wenn ich den Chat aus beruflichen Gründen nicht so verfolgen konnte, aber den Cast "gesehen" habe
[20:36:30] Dorothea_MS: Ich wünsche Euch allen einen schönen Abend!
[20:36:43] Lukas_(Protecus): dito
[20:36:47] Yusuf_Dikmenoglu: @Dorothea - Ist schon der nächste ComCast in Planung ?
[20:36:47] Lukas_(Protecus) verlässt den Chat.
[20:36:57] Dorothea_MS: Verbeug im Namen von Michael und Kay!
[20:37:05] Yusuf_Dikmenoglu: Ditoo
[20:37:17] Dorothea_MS: Ja, es stehen eine ganze Reihe von CommunityCasts an.
[20:37:27] Akiramausi: danke dorothea, dir auch einen schönen abend

[20:37:29] Dorothea_MS: Der nächste ist:

[20:37:32] Yusuf_Dikmenoglu: THX 
[20:37:47] schotti111 verlässt den Chat.
[20:38:14] Dorothea_MS: z.B. Webentwicklung mit Visual Web Developer 2005 Express Edition
[20:38:19] MaMü: Gibt es ein Ort wo man sämtlich CC angucken bzw runterladen kann?
[20:38:49] Dorothea_MS: Da kann ich Euch als Tipp geben, auf den CommunityGuide zu schauen.
[20:39:10] Dorothea_MS: Dort werden die CommunityCasts angekündigt.
[20:39:32] Dorothea_MS: Heruntergeladen werden, könnnen sie aber nur exklusiv über die präsentierenden Communities.
[20:39:35] Yusuf_Dikmenoglu: Oki Danke Dorothea
[20:39:44] MaMü: danke
[20:40:21] **Shai Hulud**: Ja Dorothea! Ich danke Dir für die gute Organisation im Vorfeld und heute.
[20:40:35] Dorothea_MS: Link zum CommunityGuide:
http://www.microsoft.com/germany/community/default.mspx
[20:40:45] Dorothea_MS: Vielen Dank für die Blumen!
[20:41:28] Akiramausi: Ich sage auch dankeschön und verabschiede mich
[20:41:33] **Shai Hulud**: Dann werde ich hier mal dicht machen!
[20:41:39] Akiramausi: euch noch einen schönen abend
[20:41:48] **Shai Hulud**: danke gleichfalls
[20:41:52] Akiramausi verlässt den Chat.
[20:41:52] Yusuf_Dikmenoglu: Dito
[20:42:04] **Shai Hulud**: Einen Schönen Abend allen hier
[20:42:18] **Shai Hulud**: Man sieht sich bei winhilfe.ch !
[20:42:19] Yusuf_Dikmenoglu: @All - einen schönen Abend noch - und bis zum nächsten Cast ;-)
[20:42:23] Dorothea_MS: Schönen abend an alle!