

Anonymous wünscht frohes Neues - Newsletter 01 / 2012

Werte Leserinnen und Leser,

war Weihnachten für Ihre IT-Infrastruktur das Fest des Friedens? Falls ja, können Sie Ihrem Schutzengel danken, denn Hacker kennen keine Feiertage. Medienstar Anonymous soll sich durch besonders rege Aktivität hervorgetan haben - natürlich im Dienste eines „guten Zwecks“, versteht sich. Doch auch unzählige weitere, tatsächlich namenlose Cyberkriminelle verfolgten ihre unlauteren Absichten unbehelligt zwischen den Jahren weiter - ohne große Publicity und indirekt unterstützt durch die urlaubsbedingt dünnere Personaldecke in den IT-Abteilungen. Aber vielleicht bieten Sie Angreifern aus dem Internet ja auch schon präventiv Paroli und sichern Ihr internes Netzwerk zugleich vor Ausspähung und Datendiebstahl - mit unserem dedizierten ReCoB-System. Es wird seit vielen Jahren kontinuierlich weiterentwickelt und schützt professionell betriebene Infrastrukturen mit der Kompetenz des weltweiten Technologieführers - unter einem Namen, der sich schnell herumspricht: TigtGate™-Pro.

Glück, Gesundheit und Erfolg im neuen Jahr wünscht Ihnen

Patrick Leibbrand
Presse und Öffentlichkeitsarbeit

P.S.:

Fragen? Anregungen? Rückmeldung? Gerne!

Schreiben Sie an: p.leibbrand@m-privacy.de. Ich freue mich auf Ihre Nachricht!

Der m-privacy-Newsletter im Januar 2012:

- 1. Top-Thema: Geliebt, gehasst und namenlos**
- 2. Aus der Entwicklungsabteilung: Weiche Schale, harter Kern**
- 3. Das war 2011 - der vorausschauende Rückblick**
- 4. „Geld her oder Daten weg!“ - was hilft gegen Ransomware?**
- 5. Tipps & Tricks: DNS Zone Forwarding**
- 6. Stichwort des Monats: Bildauflösung**
- 7. Termine und Veranstaltungen**

1 . Top-Thema: Geliebt, gehasst und namenlos

Namen sind Schall und Rauch - das hat sich die Hacker-Gruppierung „Anonymous“ offenbar zu Herzen genommen und es auf etlichen Webservern weltweit im übertragenen Sinne ordentlich rauchen lassen. Im Prinzip ist jedes Wirtschaftsunternehmen, jede Behörde eines jeden Staates, jede politische oder kommerzielle Organisation ein potenzielles Opfer all derjenigen, die ihrem Ärger auf dem Wege einer digitalen Revanche Luft machen wollen.

2 . Aus der Entwicklungsabteilung: Weiche Schale, harter Kern

Der Systemkern von TightGate™-Pro ist zwischenzeitlich in der stabilen Version 3 angekommen. Anwenderinnen und Anwender haben damit die Gewissheit, dass ihre ReCoBS-Server spätestens im Zuge des nächsten Systemupdates mit einem topaktuellen „Innenleben“ ausgestattet werden.

3 . Das war 2011 – der vorausschauende Rückblick

Für mich immer wieder faszinierend und erschreckend zugleich: die Kreativität und Versiertheit von Cyberkriminellen, mit der sie berufliche und private Computerbenutzer alltäglich mit Ihren Schadprogrammen und Angriffen überziehen. Auch das Jahr 2011 war ein Jahr der Sicherheitslücken, Angriffswarnungen und Einbruchsmeldungen - nicht das erste, nicht das spektakulärste und ganz bestimmt nicht das letzte.

4 . „Geld her oder Daten weg!“ - was hilft gegen Ransomware?

Die Idee ist alt, dreist und einfach frech: Ein Schadprogramm, etwa als E-Mail-Anhang in einem unbedachten Augenblick achtlos geöffnet, verschlüsselt wichtige Daten auf der PC-Festplatte und droht, sie ohne Zahlung eines Lösegelds nicht wieder freizugeben. Diese digitale Variante der räuberischen Erpressung kann Privatleute wie auch Gewerbetreibende in arge Bedrängnis bringen.

5 . Tipps und Tricks: DNS Zone Forwarding

Für alle Anwenderinnen und Anwender von TightGate™-Pro haben wir eine leicht nachvollziehbare Anleitung zusammengestellt, die die Einrichtung einer DNS-Zonenweiterleitung (DNS Zone Forwarding) unter Microsoft Windows Server 2003 oder 2008 beschreibt. Sie kann kostenfrei bei uns angefordert werden - E-Mail an support@m-privacy.de genügt!

6 . Stichwort des Monats: Bildauflösung

Röhrenmonitore kennen die jüngeren unter uns nur noch vom Hörensagen, die modernen Flüssigkristalldisplays werden immer größer und die Bildqualität stetig besser. Dennoch ist jede neue Gerätegeneration immer noch ein Stückchen preiswerter als die vorangegangene. Damit rückt die Frage nach der richtigen Bildauflösung wieder in den Vordergrund: Wie viele Pixel in welcher Richtung sollen es denn sein?

7 . Termine und Veranstaltungen

Die m-privacy GmbH freut sich, anlässlich der folgenden Veranstaltungen mit Ihnen in Kontakt zu treten:

25. / 26. September 2012 / Berlin, dbb forum berlin

PITS - Public IT Security

Kongress und Messe mit begleitender Fachausstellung speziell für IT-Sicherheit in der öffentlichen Verwaltung

Wir freuen uns auch über Ihren Besuch an unserem Informationsstand im Rahmen der begleitenden Fachausstellung. Die Teilnahme ist für Angehörige öffentlicher Einrichtungen und Behörden kostenfrei.

Veranstalter: Behörden Spiegel / ProPress Verlagsgesellschaft mbH

Weitere Informationen: <http://www.public-it-security.de>

16. - 18. Oktober 2012 / Nürnberg, NürnbergMesse

it-sa - Die IT-Security-Messe

Veranstalter: NürnbergMesse in Kooperation mit der SecuMedia Verlags-GmbH

Weitere Informationen: <http://www.it-sa.de>

1 . Top-Thema: Geliebt, gehasst und namenlos

Namen sind Schall und Rauch - das hat sich die Hacker-Gruppierung „Anonymous“ offenbar zu Herzen genommen und es auf etlichen Webservern weltweit im übertragenen Sinne ordentlich rauchen lassen. Zahlreiche erfolgreiche Angriffe dürften vor allem für die IT-Sicherheitsverantwortlichen der betroffenen Firmen und Organisationen indes einer schallenden Ohrfeige gleichkommen. Interessanterweise werden die vorgeblich politisch motivierten Einbrüche in IT-Systeme ebenso wie die damit verbundene Manipulation teils kritischer Systeme oder der Diebstahl sensibler Daten nicht grundsätzlich negativ aufgenommen.

Es scheint, als sei der an sich kriminelle Akt des vorsätzlich unbefugten Eindringens in datentechnische Anlagen unter gewissen Umständen durchaus konsens- und zustimmungsfähig. Sollte hieraus zu folgern sein, dass ein vermeintlich guter Zweck jedes fragwürdige Mittel heiligt, müsste man entsprechend die negative Grundstimmung gegen „offizielle“ Verfahren zur verdeckten Unterminierung gegnerischer Infrastrukturen à la Bundestrojaner unter ganz neuen Gesichtspunkten diskutieren. Vertraut man einem dubiosen Konsortium selbst ernannter Robin Hoods mehr als der eigenen, demokratisch legitimierte Regierung?

Das Phänomen ist nicht wirklich neu - längst hat sich der Begriff des „Hacktivisten“ für diese Spezies illegaler Datenkrieger etabliert. Ob Anonymous, LulzSec oder No Name Crew: unter sicherheitstechnischen Aspekten verschwimmen die Unterschiede ebenso wie die persönlichen Beweggründe einzelner Protagonisten, die gelegentlich nach aufwendigen Ermittlungen festgenommen werden. Es verbleibt ein beträchtlicher, multidimensionaler Schaden als Folge des Ausfalls wichtiger Rechnersysteme oder durch „Leakage“ interner Datenbestände.

Mit Cyberkriminalität ist es ganz ähnlich wie mit dem „analogen“ Verbrechen, das uns im täglichen Leben häufig begegnet: niemand kann mit Sicherheit sagen, wen es als nächstes trifft. Im Prinzip ist jedes Wirtschaftsunternehmen, jede Behörde eines jeden Staates, jede politische oder kommerzielle Organisation ein potenzielles Opfer all derjenigen, die ihrem Ärger auf dem Wege einer digitalen Revanche Luft machen wollen. Das Internet ist dafür ein ideales Vehikel, denn es erreicht mittlerweile so gut wie jeden. Jeder, von der Privatperson bis hin zum Großkonzern, muss gezwungenermaßen Wege finden, Angreifern die Stirn zu bieten.

Leider sind die Möglichkeiten der schädlichen Einwirkung aus dem Internet auf dort „sichtbare“ oder zugängliche IT-Systeme ungleich größer als die einer effektiven Verfolgung der Täter auf demselben Weg. Man kann getrost von einer asymmetrischen Bedrohung sprechen, weswegen präventiven Maßnahmen zur Gefahrenabwehr eine besondere Bedeutung zukommt. „Vorbeugen ist besser als heilen!“, sagen sich Systemadministratoren weltweit und nehmen jeden auch nur teilweise erfolgreichen Angriff auf ihre Webserver zum Anlass, die getroffenen Sicherheitsvorkehrungen zu überprüfen und erforderlichenfalls zu optimieren.

Dieser Präventivgedanke greift mehr und mehr auch im Hinblick auf die Absicherung interner Netzwerke in Industriebetrieben oder Einrichtungen der öffentlichen Verwaltung. In heutiger Zeit sind die einzelnen Arbeitsplatzrechner viel zu häufig noch mehr oder weniger unmittelbar mit dem offenen Internet verbunden, allenfalls konventionell durch Virens Scanner und Firewalls geschützt. Nach und nach setzt sich die Erkenntnis durch, dass das zumindest in kritischen Umgebungen mit erhöhtem Schutzbedarf nicht mehr ausreicht.

Eine triviale Sicherheitslücke im Internetbrowser eines einzigen Arbeitsplatzcomputers kann bereits große Teile des internen Netzwerks exponieren und offeriert sensible Firmendaten quasi zur Selbstbedienung für Unbefugte. IT-Verantwortliche für Bereiche mit erhöhtem Schutzniveau entscheiden sich daher zusätzlich für eine physikalische Trennung des internen Firmen- oder Behördennetzwerks vom offenen Internet. Der früher unvermeidliche Aufwand einer doppelten Infrastruktur zur gleichzeitigen Nutzung interner und externer Ressourcen kann heute glücklicherweise vermieden werden.

Mittels Remote-Controlled Browser Systems (ReCoBS) wie TightGate™-Pro kommuniziert der Browser auf dem Arbeitsplatzrechner nicht mehr direkt mit dem Internet. Stattdessen übernimmt der dem internen Netzwerk vorgelagerte ReCoBS-Server die Ausführung des Browsers. Das System ruft die angeforderten Web-Daten ab und leitet dem Computer des Anwenders nur die Bildschirmausgabe zu. Sicherheitslücken, die Hacker aller Couleur mit oft erstaunlicher Detailkenntnis ausnutzen, können sich

auf das interne Netzwerk nicht mehr auswirken. Zugleich bleibt die Internetfunktionalität eines jeden Arbeitsplatzrechners voll erhalten, selbst aktive Inhalte und Multimediaapplikationen sind gefahrlos nutzbar. Auch Arbeitsplätze, die bislang aus Sicherheitsüberlegungen heraus nicht entsprechend angebunden waren, können über ein dediziertes ReCoBS von der Produktivitätssteigerung eines Internetanschlusses profitieren.

Stichwort Data Leakage: Durch die physikalische Trennung haben auch bereits auf anderen Wegen in das interne Netzwerk gelangte Schadprogramme keine Chance, sensible Daten über das Internet zu versenden. Ein funktionsspezifisches Protokoll zwischen ReCoBS-Server und internem Netzwerk sowie der massive Eigenschutz des vorgeschalteten Schutzsystems lassen auch gezielte Hackerangriffe ins Leere laufen. Abstand schafft Sicherheit in jeder Hinsicht - auch und gerade bezüglich der vielen namenlosen Gefahren aus dem „Netz der Netze“.

Erfahren Sie mehr:

So funktioniert der Angriff via Webbrowser:

http://www.m-privacy.de/produkte/tightgate_pro/szenario

Alles über TightGate™-Pro:

<http://www.m-privacy.de/produkte/tightgate-pro/>

Die TightGate™-Technologie: Was steckt dahinter?

<http://www.m-privacy.de/unternehmen/technologie>

heise.de: Anonymous greift Sicherheitsberater an

<http://heise.de/-1401351>

heise.de: FBI nimmt mutmaßlichen LulzSec-Hacker fest

<http://heise.de/-1348877>

2 . Aus der Entwicklungsabteilung: Weiche Schale, harter Kern

Viele Köche verderben den Brei? Nicht unbedingt: Im Fall des quelloffenen Betriebssystems Linux gilt sogar das Gegenteil. Eine weltweite Entwicklungsgemeinde leistet ihre Beiträge zu diesem fortwährend evolvierenden Projekt, verändert und verbessert es. Hunderte Augen sichten den für jedermann frei verfügbaren Quellcode quasiparallel nach Fehlern und zahlreiche, bisweilen namhafte Experten nehmen Ergänzungen und Korrekturen vor. Diese einmalige Konstellation prädestiniert Linux geradezu zur Implementierung kritischer Applikationen. Auch wir nutzen eine speziell sicherheitsoptimierte Variante von Debian-Linux als Basis für unsere dedizierten ReCoB-Systeme. Deren Systemkern ist zwischenzeitlich in der stabilen Version 3 angekommen. Anwenderinnen und Anwender von TightGate™-Pro haben damit die Gewissheit, dass ihre ReCoBS-Server spätestens im Zuge des nächsten Systemupdates mit einem topaktuellen „Innenleben“ ausgestattet werden. Trotz des neuen, „harten“ Kerns bleiben Funktionalität und Benutzerfreundlichkeit natürlich wie gewohnt erhalten.

Apropos Innenleben: Wussten Sie, dass Sie sich mit wenigen Handgriffen und ganz ohne Aufruf der umfangreichen Konfigurationsmenüs eine schnelle Übersicht der Systemfunktionen Ihres TightGate™-Pro-Servers verschaffen können? Hierzu gibt es die Statusseiten, die Sie ganz einfach als angemeldeter VNC-Benutzer durch Aufruf der URL <http://localhost> einsehen können. Einzige Voraussetzung ist die einmalige Erteilung der diesbezüglichen Berechtigung durch den Administrator config. Wir haben die Statusseiten in der kommenden Version von TightGate™-Pro noch benutzerfreundlicher gestaltet und die relevanten Informationen übersichtlicher gegliedert. Anhand leicht erfassbarer Farbfelder sehen Sie auf einen Blick: Alles im grünen Bereich.

Unser Tipp, damit das ohne viel Aufwand auch immer so bleibt: Auto-Update-Funktion einschalten!

Erfahren Sie mehr:

ReCoB-Systeme in der Praxis:

<http://www.m-privacy.de/unternehmen/technologie/recobs>

TightGate™-Pro im Detail:

<http://www.m-privacy.de/produkte/tightgate-pro>**3 . Das war 2011 – der vorausschauende Rückblick**

Für mich immer wieder faszinierend und erschreckend zugleich: die Kreativität und Versiertheit von Cyberkriminellen, mit der sie berufliche und private Computerbenutzer alltäglich mit Ihren Schadprogrammen und Angriffen überziehen. Auch das Jahr 2011 war ein Jahr der Sicherheitslücken, Angriffswarnungen und Einbruchsmeldungen - nicht das erste, nicht das spektakulärste und ganz bestimmt nicht das letzte. Aber wieder einmal ein Jahr, das bei konsequenter Anwendung aller verfügbarer Abwehrmaßnahmen weitaus ereignisärmer hätte ausfallen können. Hätte können.

Bei Licht betrachtet müsste die Kombination aus fortschrittlicher Technik und gut geschultem Personal eine schier unüberwindliche Hürde für die Angreifer darstellen, die es auf unterschiedlichen Wegen auf Daten, Systeme und Netzwerke abgesehen haben. Doch das Gegenteil scheint der Fall. Verfolgt man die Berichterstattung, so gewinnt man den Eindruck, als nähme der Erfolg von Hackern und Datendieben mit steigendem Angriffsdruck weltweit stetig zu. Der Chaos Computer Club (CCC) spricht von „immer schwierigerer Datenhygiene“ und sagt wenig durchgreifende Verbesserungen für 2012 voraus.

Dabei ist es viel einfacher als oft angenommen, IT-Sicherheit erfolgreich in die eigenen Hände zu nehmen. Es gibt keinen belegbaren Grund, sich von düsteren Prophezeiungen einschüchtern zu lassen. Die bereits heute möglichen Gegenmaßnahmen können durchaus stärker sein als der perfideste Angriff! Man mag einwenden, dass sich die grundsätzliche Schwachstelle „Mensch“ auch in sicherheitstechnisch hochgerüsteten IT-Infrastrukturen nicht völlig eliminieren lässt. Das stimmt sicherlich, doch motivierte Mitarbeiter auf hohem Awareness-Level kombiniert mit Schutzsystemen mit möglichst großer Präventivwirkung bannen praktisch jede digitale Gefahr.

Betreiber professionell genutzter Infrastrukturen setzen von jeher auf umfangreiche technische Sicherungsmaßnahmen. In manchen Fällen steht der Security-Gedanke so weit im Vordergrund, dass Überlegungen zur Wirtschaftlichkeit dahinter zurückstehen. Häufig spielt jedoch Geld durchaus eine Rolle, wenn es um die Umsetzung einer adäquaten Sicherheitsstrategie in Unternehmen oder Behörden geht. Systemverantwortliche stehen dann vor der Herausforderung, ihren tatsächlichen Bedarf exakt zu ermitteln, verfügbare Systeme zielorientiert zu evaluieren und letztlich die Lösung mit dem besten Preis-/Leistungsverhältnis aus der Vielzahl von Angeboten auszufiltern.

Gerade die so genannten Remote-Controlled Browser Systems (ReCoBS) werden meist zu Unrecht als zu komplex und kostspielig bewertet. In wirtschaftlich angespannten Zeiten fällt die Entscheidung zugunsten dieser hoch entwickelten Systeme nicht immer leicht, obgleich deren herausragende Wirksamkeit gegen Angriffe auf interne Netzwerke aus dem Internet in Fachkreisen unbestritten ist. Den notwendigen Informationstransfer hin zu Entscheidungsträgern in technischen und betriebswirtschaftlichen Bereichen unterstützen wir daher nach Kräften. Unzählige Varianten der immer gleichen Angriffsprinzipien haben uns in der vergangenen Monaten beschäftigt. Einige davon haben wir in unseren Newslettern für Sie genauer beleuchtet, um den hohen praktischen Nutzen dedizierter Schutzsysteme zu verdeutlichen.

Lässt man die Sicherheitsvorfälle des abgelaufenen Jahres Revue passieren, so fällt auf: ReCoB-Systeme wie TightGate™-Pro helfen vor allem gegen die besonders oft auftretenden Bedrohungen – und das vorbeugend und damit sehr zuverlässig. Da wäre zunächst die Paradedisziplin eines ReCoBS, die präventive Verhinderung eines Angriffs auf interne Infrastrukturen über Sicherheitslücken lokal installierter Webbrowser. Es lässt sich nicht beziffern, in wie vielen Fällen TightGate™-Pro unsere Kunden vor Schäden und Datenverlust bewahrt hat. Aber: Nach der Einführung von TightGate™-Pro kam es zu keinem erfolgreichen Angriff mehr, in Anbetracht wöchentlich neu entdeckter und aktiv ausgenutzter Schwachstellen eine sehr positive Bilanz. Zuvor stellte sich diese Situation trotz des Einsatzes konventioneller Abwehrmaßnahmen weniger erfreulich dar.

Darüber hinaus begegnet ein ReCoBS wie TightGate™-Pro einer Vielzahl unerwünschter und gefährlicher Seiteneffekte, die sich in Zeiten globaler Vernetzung kaum ausschließen lassen. Nachhaltiger Schutz ist dagegen leicht erreichbar: Webinhalte, die über einen ferngesteuerten Internetbrowser abgerufen werden, werden ausschließlich auf dem vorgeschalteten Schutzsystem und damit außerhalb des internen Netzwerks verarbeitet. Drive-by-Downloads von Malware werden unmöglich, ebenso wie deren unbemerkte Installation auf einzelnen Arbeitsplatzrechnern. Gleiches gilt für die von vielen Systemadministratoren argwöhnisch betrachteten aktiven Inhalte - ganz zu schweigen von Adobe Flash, einer wegen zahlreicher Sicherheitsprobleme auffallend oft kritisierten Technologie.

Ein Remote-Controlled Browser System steigert das Sicherheitsniveau des internen Netzwerks signifikant – zugleich bleibt die Internetfunktionalität eines jeden Arbeitsplatzes vollständig erhalten. Letzterer muss zur Verbindung mit TightGate™-Pro lediglich mit zwei lizenzkostenfreien Mini-applikationen ausgerüstet werden – umfangreiche oder systemnahe Softwareinstallationen sind nicht notwendig. Von komplizierter Handhabung kann also keine Rede sein, zumal der eigentliche ReCoBS-Server als betriebsbereit vorkonfigurierte Appliance geliefert wird. Und wer Einrichtung und Administration unseres ReCoBS-Flaggschiffs beispielsweise im Rahmen einer Teststellung einmal selbst erlebt hat, sieht in Anbetracht der Zeit- und Ressourcenersparnis im Vergleich zu sicherheitstechnisch weit weniger effektiven Alternativen auch den Preis mit ganz anderen Augen.

An dieser Stelle schlagen wir die trüben Prognosen des CCC guten Gewissens in den Wind: Das Jahr 2012 hat für unsere Kunden und Partner die besten Voraussetzungen, ein rundweg gutes Jahr zu werden. Begründeter Anlass zum Optimismus sozusagen!

Erfahren Sie mehr:

So funktioniert der Angriff via Webbrowser:

http://www.m-privacy.de/produkte/tightgate_pro/szenario

Die TightGate™-Technologie: Was steckt dahinter?

<http://www.m-privacy.de/unternehmen/technologie>

golem.de: Datenhygiene wird immer schwieriger

<http://www.golem.de/1112/88727.html>

4 . „Geld her oder Daten weg! - Was hilft gegen Ransomware?

Die Idee ist alt, dreist und einfach frech: Ein Schadprogramm, etwa als E-Mail-Anhang in einem unbedachten Augenblick achtlos geöffnet, verschlüsselt wichtige Daten auf der PC-Festplatte und droht, sie ohne Zahlung eines Lösegelds nicht wieder freizugeben. Diese digitale Variante der räuberischen Erpressung kann Privatleute wie auch Gewerbetreibende in arge Bedrängnis bringen, etwa wenn kein aktuelles Backup der so „auf Eis“ liegenden Daten zur Verfügung steht oder wichtige Arbeitsmittel wie Rechnerarbeitsplätze blockiert werden.

In der Regel erreicht die so genannte „Ransomware“ (Kunstwort aus engl. „ransom“ = Lösegeld und „software“) den Rechner eines potenziellen Opfers in Form eines Trojaners. Der Schadcode tarnt sich also als Anwendung, PDF-Datei, Programmaktualisierung oder anderweitig nützliche bzw. erforderliche Programmkomponente. Zugleich versuchen Cyberkriminelle mit Akribie und Perfektionismus, den Anwender durch unterschiedliche Social-Engineering-Vorgehensweisen zur Ausführung der Applikation zu bewegen.

Wie bei Erpressungsversuchen üblich, lässt sich das Problem in keinem Fall durch Zahlung des geforderten Betrags aus der Welt schaffen. In vielen Fällen erfolgt dann letztlich dennoch keine Freigabe der verschlüsselten Daten, es kann zu weitergehenden Forderungen der Erpresser kommen und überdies sind die Verfahren zur Blockade der Opferrechner in vielen Fällen eher trivial. Gute Gründe also, sich nicht ins Bockshorn jagen zu lassen und den befallenen Rechner stattdessen mit einer startfähigen CD und einem darauf befindlichen, aktuellen Antivirenprogramm zu „desinfizieren“.

Nervenschonender und kostengünstiger ist es allemal, schon im Vorfeld derartiger Attacken geeignete Schutzvorkehrungen zu treffen. „Ransomware“ ist grundsätzlich gewöhnliche Malware, gegen die alltagsbewährte Abwehrmaßnahmen meist zuverlässig wirkt. Wer sich nicht allein auf reaktive, d. h. filternde Systeme wie Virens Scanner oder Firewalls mit ihren spezifischen Nachteilen verlassen will,

greift zu vorgeschalteten Schutzsystemen mit besonders ausgeprägter Präventivwirkung.

Das dedizierte ReCoB-System TightGate™-Pro schützt nicht nur den Arbeitsplatz-PC und das ihn umgebende interne Netzwerk vor Angriffen aus dem Internet, sondern kann auch eine Vielzahl von Dateitypen auf dem vorgelagerten Schutzsystem öffnen und verarbeiten. Selbst der Empfang von E-Mail ist damit außerhalb des internen Firmen- oder Behördennetzwerks möglich. So können etwa Anhänge oder Downloads in Augenschein genommen werden, ohne interne Infrastrukturen der Gefahr einer Kompromittierung oder böswilligen Veränderung auszusetzen. Schädliche Inhalte werden erkannt und blockiert, ohne dass sie den Arbeitsplatzrechner überhaupt erreichen.

Erfahren Sie mehr:

Wikipedia: Ransomware

<http://de.wikipedia.org/wiki/Ransomware>

heise.de: Schadsoftware nach Landessitte

<http://heise.de/-1398669>

5 . Tipps und Tricks: DNS Zone Forwarding

Leistungsstarke ReCoB-Systeme der TightGate™-Pro-Produktlinie werden aus Kapazitätsgründen stets als Rechnerverbund (Cluster) ausgeführt. Dieser Rechnerverbund besteht aus mehreren Einzelrechnern, die „Nodes“ genannt werden. TightGate™-Pro verfügt über eine automatische Lastverteilung. Diese Lastverteilung, auch „Load Balancing“ genannt, ist die Grundlage eines optimierten Systembetriebs. Je nach aktueller Beanspruchung der einzelnen Nodes werden neue Verbindungsanfragen an den jeweils am wenigsten belasteten Rechner des Verbunds übergeben.

In jedem TightGate™-Pro-Cluster sind in Abhängigkeit von der Gesamtzahl der Einzelrechner mehrere der Nodes zusätzlich zu ihren eigentlichen Aufgaben als Load Balancer im Einsatz. Sie prüfen in kurzen Abständen die Belastungssituation im Rechnerverbund und entscheiden bei einer Verbindungsanfrage, welcher Node die neue Benutzersitzung übernehmen wird.

Damit die Lastverteilung einwandfrei arbeitet, dürfen die einzelnen Rechner im Verbund seitens der Klientenrechner nicht dediziert über deren IPv4-Adresse angesprochen werden. Stattdessen muss der gesamte TightGate™-Pro-Cluster im internen Netzwerk als Einheit erscheinen. Zusätzlich sind alle neuen Verbindungsanfragen zunächst an die Nodes zu übermitteln, welche die Aufgabe der Lastverteilung wahrnehmen.

Dies wird erreicht, indem die Verbindungsanfragen an einen zentralen Rechnernamen gestellt werden, der den Rechnerverbund repräsentiert. Die separate DNS-Zone für den TightGate™-Pro-Cluster nimmt die einzelnen Nodes des ReCoB-Systems aus der Verwaltung des lokalen DNS-Servers aus. Stattdessen übernimmt die Lastverteilung von TightGate™-Pro die interne Adresskoordination des TightGate™-Pro-Rechnerverbunds entsprechend der aktuellen Lastsituation.

Für alle Anwenderinnen und Anwender von TightGate™-Pro haben wir eine leicht nachvollziehbare Anleitung zusammengestellt, die die Einrichtung einer DNS-Zonenweiterleitung (DNS Zone Forwarding) unter Microsoft Windows Server 2003 oder 2008 beschreibt. Sie kann kostenfrei bei uns angefordert werden - E-Mail an support@m-privacy.de genügt!

6 . Stichwort des Monats: Bildauflösung

Bis vor einigen Jahren fristete der Begriff der Bildauflösung auch bei technikaffinen Zeitgenossen eher ein Schattendasein. Das hat sich erst mit zunehmender Verbreitung digitaler Fotokameras grundlegend geändert. Die zunächst vorherrschende Meinung des „viel hilft viel“ hat sich zwar bald als falsch herausgestellt, doch wissen zwischenzeitlich immer mehr Anwenderinnen und Anwender etwas mit dem Terminus anzufangen.

Insbesondere bei der Mensch-Maschine-Schnittstelle schlechthin, dem Bildschirm oder Computermonitor, ist die Bildauflösung von besonderer Bedeutung im Hinblick auf Funktionalität und Ergonomie. Dennoch interessierte man sich in den Büros oder Privathaushalten lange Zeit eher wenig für diesen Parameter. Der Grund war einfach: Es gab nur wenig Auswahl hinsichtlich verfügbarer und auch er-

schwinglicher Alternativen. Zwar boten die Sichtgeräte früherer Jahre verglichen mit den jetzt erhältlichen Lösungen in Sachen Bildqualität generell ein aus heutiger Sicht inakzeptables Qualitätsniveau. Doch man war gezwungenermaßen zufrieden mit dem, was man auf seinem Schreibtisch hatte.

Der Preisverfall bei der aktuellen Displaytechnologie ist in diesem Zusammenhang nicht nur arbeitsmedizinisch ein wahrer Segen. Röhrenmonitore kennen die jüngeren unter uns nur noch vom Hörensagen, die modernen Flüssigkristalldisplays werden immer größer und die Bildqualität stetig besser. Dennoch ist jede neue Gerätegeneration immer noch ein Stückchen preiswerter als die vorangegangene. Damit rückt die Frage nach der richtigen Bildauflösung wieder in den Vordergrund: Wie viele Pixel in welcher Richtung sollen es denn sein?

Vieles bleibt Geschmackssache, aber für manche Aspekte lassen sich gute Faustformeln und für einige auch klare Regeln angeben. Generell sollte man wissen, dass Flachbildschirme eine fest definierte, bauartbedingte Bildauflösung aufweisen. Damit unterscheiden sie sich grundlegend von den heute ungebräuchlichen Monitoren mit Kathodenstrahlröhre. Dies bedeutet jedoch auch: Ein einwandfreies Bild erhält nur, wer seinen Bildschirm mit genau dieser „Eigenauflösung“ ansteuert und nicht etwa willkürlich einen anderen Wert in den Systemeinstellungen der Grafikkarte auswählt. Monitor und Rechner kommunizieren miteinander - der automatisch ausgehandelte Wert für die Bildauflösung ist in aller Regel optimal. Manuelle Anpassungen kommen allenfalls in Spezialfällen in Betracht, etwa zur Ansteuerung eines Projektors mit abweichender Auflösung.

Welche Bildschirmgröße infrage kommt, mag man anhand seiner hauptsächlichen Anwendungsszenarien und dem Platzangebot auf dem eigenen Schreibtisch entscheiden. Unter 19“ (Zoll) wird man heute kaum noch ein modernes Sichtgerät erhalten. Diese Bildschirme stellen mindestens 1280 x 1024 Bildpunkte dar, was allerdings für manche Applikationen wie Tabellenkalkulation oder Bildbearbeitung bereits zu wenig sein kann. Fehlt es an Bildschirmfläche, muss ein größerer Monitor her.

Allerdings sollte man dann darauf achten, dass auch die verfügbare Bildauflösung steigt. Das ist leider nicht immer der Fall. Displays mit geringerer Auflösung können trotz größerer Schirmfläche weitaus billiger gefertigt werden, das verleitet so manchen Hersteller zum „Schummeln“. Mein Tipp: Das „Elektronik-Kompendium“ (siehe Link) bietet eine gute Übersicht über sinnvolle Kombinationen von sichtbarer Bildschirmfläche und Bildauflösung. Liegen die Daten Ihres Wunschmonitors in einer der grau unterlegten Zeilen, ist funktional und ergonomisch alles in Ordnung.

Sollten Ihnen die Bedienelemente Ihrer Benutzeroberfläche oder die Schriften auf dem Bildschirm dennoch zu klein oder zu groß vorkommen, so widerstehen Sie bitte der Versuchung, diesem Makel mit einer Veränderung der Bildauflösung beizukommen. Wie eingangs erwähnt, leidet darunter die Anzeigequalität erheblich. Passen Sie stattdessen die Schriftdarstellung in der entsprechenden „Systemsteuerung“ an - alle modernen Betriebssysteme bieten Ihnen hierzu weitreichende Möglichkeiten.

TightGate™-Pro hält in Sachen Bildauflösung übrigens ein besonderes Bonbon für Sie bereit: den stufenlos skalierbaren Viewer! Obwohl der Browser bei TightGate™-Pro auf einem vorgeschalteten Schutzsystem ausgeführt wird und Sie lediglich dessen Bildschirmausgabe über ein Viewer-Programm sehen, müssen Sie auf den gewohnten Komfort beim Surfen nicht verzichten. Ziehen Sie sich das Viewer-Fenster einfach mit der Maus auf die gewünschte Größe - in wenigen Augenblicken wird die Darstellung automatisch an die neue Fensterdimensionen angeglichen. Sie haben sogar eine moderne Doppelmonitoranlage? Umso besser: Dann verschieben Sie einfach das Viewer-Fenster auf einen eigenen Bildschirm und maximieren Sie es dort (Vollbilddarstellung) - für maximales Surfvergnügen!

Erfahren Sie mehr:

Wikipedia: Bildauflösung

<http://de.wikipedia.org/wiki/Bildauf%C3%B6sung>

Elektronik-Kompendium: Bildschirmgröße und Auflösung

<http://www.elektronik-kompendium.de/sites/com/0808181.htm>

7 . Termine und Veranstaltungen

Die m-privacy GmbH freut sich, anlässlich der folgenden Veranstaltungen mit Ihnen in Kontakt zu treten:

25. / 26. September 2012 / Berlin, dbb forum berlin

PITS - Public IT Security

Kongress und Messe mit begleitender Fachausstellung speziell für IT-Sicherheit in der öffentlichen Verwaltung

Wir freuen uns auch über Ihren Besuch an unserem Informationsstand im Rahmen der begleitenden Fachausstellung. Die Teilnahme ist für Angehörige öffentlicher Einrichtungen und Behörden kostenfrei.

Veranstalter: Behörden Spiegel / ProPress Verlagsgesellschaft mbH

Weitere Informationen: <http://www.public-it-security.de>

16. - 18. Oktober 2012 / Nürnberg, NürnbergMesse

it-sa - Die IT-Security-Messe

Veranstalter: NürnbergMesse in Kooperation mit der SecuMedia Verlags-GmbH

Weitere Informationen: <http://www.it-sa.de>