pallas

eco Verband der deutschen Internetwirtschaft e.V.

Arbeitskreis Sicherheit

Veranstaltung:

Sitzung am 06. Mai 2009, Köln

Thema: Sicherheit in der Gesundheitstelematik

Leitung:

Dr. Kurt Brand

Geschäftsführer Pallas GmbH

Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

information (at) pallas.de
http://www.pallas.de

Der (digitale) Wurm im Krankenhaus

heise Security

Sie sind Gast
Einloggen | Registrieren

Suche
los
Im Browser einrichten

News
7-Tage-Alerts
7-Tage-News
News-Archiv
Newsletter
English News
RSS-Feed

Anzeige

Hintergrund
BSI-Info
Know-how
Kommentar

News

Meldung vom 03.02.2009 11:02 [<< Vorige] [Nächste >>]

Fehlkonfiguration erleichterte Wurmausbruch in Londoner Krankenhäusern vorlesen

Die Infektion der Computersysteme von drei Londoner Krankenhäusern im November 2008 mit dem Windows-Wurm Mytob ist laut einem Untersuchungsbericht größtenteils auf eine Fehlkonfiguration zurückzuführen gewesen. So habe es zwar einen Virenschutz gegeben, der auch täglich aktualisiert wurde, allerdings hätten die Updates nicht alle PCs erreicht. Zudem sei die Antiviren-Software auf einigen der rund 4700 Systeme falsch konfiguriert gewesen, was eine Hintertür für den seit mehr als drei Jahren bekannten Wurm offen gelassen habe. Genauere Angaben macht der Bericht nicht. Medienberichten zufolge soll es sich bei der Antivirensoftware um VirusScan Enterprise von McAfee handeln.

Die drei zusammen gehörenden Krankenhäuser St. Bartholomew's, the Royal London Hospital und The London Chest Hospital waren durch die Infektion der PCs gezwungen, auf einen Notbetrieb umzusteigen. Die Patientenaufnahme habe zwar weiterhin funktioniert, Notfälle seien damals aber sicherheitshalber zu anderen Krankenhäusern weitergeleitet worden. Der Wurm habe keine Schäden angerichtet und keinen Zugriff auf Patientendaten gehabt.

Der nur teilweise öffentlich verfügbare Abschlussbericht empfiehlt unter anderem, das Personal zusätzlich zu schulen, um das Risiko für weitere Attacken zu senken.

Siehe dazu auch:

- Computervirus legt Netzwerke in Londoner Krankenhäusern lahm, Bericht auf heise Security

(dab/c't)

Patientenschutz schützt Conficker gleich mit

heise Security

Sie sind Gast
Einloggen | Registrieren

Suche
los
Im Browser einrichten

News
7-Tage-Alerts
7-Tage-News
News-Archiv
Newsletter
English News
RSS-Feed

Anzeige

Hintergrund
BSI-Info
Know-how
Kommentar
Praxis
Produkte

News

Meldung vom 03.05.2009 12:37

[<< Vorige] [Nächste >>]

Bürokratie verhindert die Reinigung virenverseuchter medizinischer Computer

vorlesen

Vom Conficker-Virus befallene Rechner im medizinischen Einsatz in verschiedenen US-Kliniken konnten aufgrund staatlicher Vorschriften nicht unverzüglich von der Schadsoftware befreit werden. Der Fall heizt die Diskussion um das von der US-Regierung forcierte Programm für mehr Cybersicherheit weiter an.

Wie Rodney Joffe, einer der Gründer der Conficker Working Group, gegenüber dem Nachrichtensender *CBS* erklärte, seien die betroffenen Computer unter anderem für die Berechnung und Analyse von Bildern in der Magnet-Resonanz-Tomografie (MRT) verwendet worden. Speziell für das Gesundheitswesen ausgearbeitete Vorschriften, die eigentlich dem Schutz von Patienten und Ärzten gelten, hielten die Krankenhäuser jedoch davon ab, die infizierten Rechner zu reinigen – in derartigen Fällen gelten Wartefristen von bis zu 90 Tagen, bevor die Systeme "manipuliert" werden dürften.

Den Behörden teilte Joffe mit, seine Organisation habe in den vergangenen drei Wochen über 300 kritische medizinische Systeme ausgemacht, die allesamt infiziert seien und alle vom gleichen Hersteller stammten. Die Rechner seien zudem vielfach nicht nur in unmittelbarer Nähe oder sogar direkt auf Intensivstationen der Kliniken im Einsatz, sondern außerdem über lokale Netzwerke mit dem Internet verbunden. Derart kritische Systeme dürften keinesfalls an das Internet gekoppelt werden, warnte Joffe.

Joffe lehnte in diesem Zusammenhang auch die Pläne der Obama-Regierung für ein neues US-Stromnetz ab. Wie eine Studie des US-Sicherheitsunternehmens IOActive gezeigt hatte, weisen die für den dortigen Einsatz geplanten Systeme erhebliche Sicherheitslücken auf, die Cyberattacken Tür und Tor öffnen könnten. Joffe wiederholte daher seine Forderungen, das U.S. Computer Emergency Readiness Team des Department of Homeland Security als Aufsichtsbehörde für Cybersecurity sowohl personell wie auch finanziell in die Lage zu versetzen, seine Aufgabe erfüllen zu können – unter der Kontrolle durch die Regierung. (map/c't)

Lösegeld für 8 Mio Patienten(daten)

heise Security

Sie sind Gast
Einloggen | Registrieren

Suche
los
Im Browser einrichten

News
7-Tage-Alerts
7-Tage-News
News-Archiv
Newsletter
English News
RSS-Feed

News

Meldung vom 05.05.2009 12:01

[<< Vorige] [Nächste >>]

Cracker fordern 10 Millionen US-Dollar für Patientendatenbank

vorlesen

Kriminelle sollen US-Medienberichten zufolge die Daten von 8 Millionen amerikanischen Schmerzpatienten vom Server des Virginia Prescription Monitoring Program gestohlen haben und nun 10 Millionen US-Dollar Lösegeld fordern. Der Server dient Ärzten zur Überwachung der Herausgabe von Rezepten für Schmerzmittel wie Opiate und soll den Drogenmissbrauch verhindern.

Nach Angaben von Brian Krebs von der Washington Post drangen die Kriminellen auf unbekanntem Weg in den Server ein, verschlüsselten die Daten, löschten die Originale anschließend auf dem Server und hinterließen den Erpresserbrief. Dieser wurde auch auf Wikileaks veröffentlicht:

"I have your shit! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uhoh :(For $10 million, I will gladly send along the password."

Der Server ist derzeit nicht mehr erreichbar. Nach Angaben des Virginia's Department of Health Professions sind die Ermittlungsbehörden bereits eingeschaltet. (dab/c't)

Agenda

13:00	Registrierung
13:30	**Begrüßung und Vorstellung NetCologne** Ivan Andric, Leiter Systemberatung *NetCologne GmbH*
13:45	**Datenschutz und IT-Sicherheit: Empfehlungen von BÄK und KBV für Ärzte** Dr. med. Dipl.-Inform. Georgios Raptis, Referent Telematik / IT-Sicherheit *Bundesärztekammer*
14:30	**Sichere Telematikanwendungen der eGK** Sven Marx, Leiter Datenschutz und Informationssicherheit *gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH*
15:15	**Kaffeepause und Networking**
15:45	**Geschäftsmodelle für IT-Sicherheit im Gesundheitswesen** Frank Bodenstein, Business Development Manager *DGN Deutsches Gesundheitsnetz Service GmbH*
16:30	**Aufbau einer hoch sicheren eHealth-Infrastruktur in Baden-Württemberg** Jörg Stadler, Head of eHealth Infrastructure Product House Dr. Jens Urmann, Product Management Security *InterComponentWare AG*
17:15	**Die aktuelle Lage im Sicherheitsbereich** Dr. Kurt Brand, Arbeitskreisleiter Sicherheit und Geschäftsführer *Pallas GmbH*
17:30	**Verschiedenes, Themen und Termine**

pallas

Aktuelle Lage im

Sicherheitsbereich

Veranstaltung:

Sitzung am 06. Mai 2009, Köln

Thema: Sicherheit in der Gesundheitstelematik

Referent:

Dr. Kurt Brand

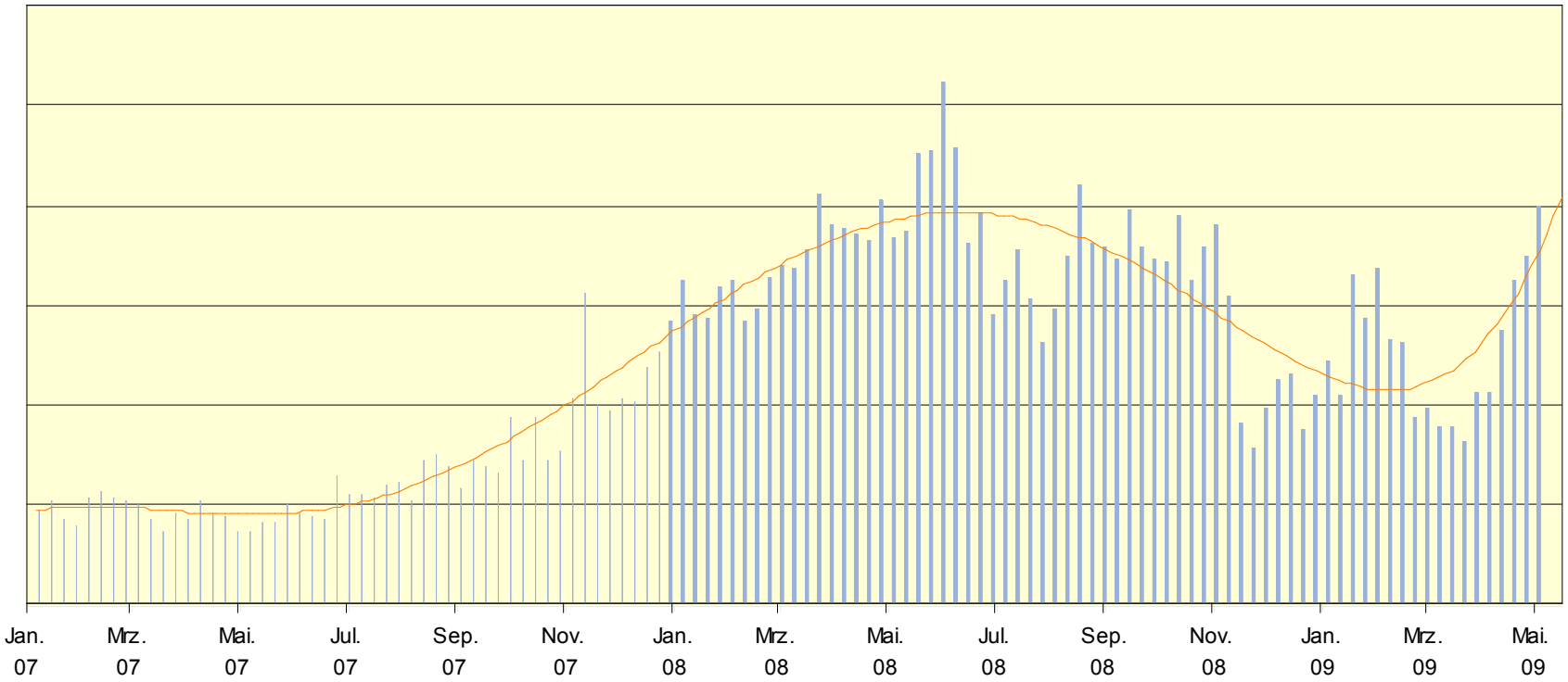
Geschäftsführer Pallas GmbH

Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

information (at) pallas.de
http://www.pallas.de

MySpam

- Letztes Wochenende Top-10-Wert
- Steilster Anstieg letzte 6 Wochen



Wichtige Security-News, letzte drei Monate 1/2

- Erste Anzeichen für Botnetz aus Macs
- Hälfte der Datenlecks: Verlust/Klau von PCs und Datenträgern
- Starker Anstieg der Malware-Verbreitung über Wechselmedien
- 5 % der Untenehmens-PCs sind Bots (fehlender Real-Time-Schutz)
- Neues Botnetz mit 2 Mio Rechnern durch manipulierte Webseiten erzeugt
- 9 Mio US $ mit geklonten Kreditkarten in weltweitem Coup an einem einzigen Tag an Bankautomaten abgehoben
- Kinderporno-Stoppseiten: BKA überwacht Zugriffe in Echtzeit?
- Secureworks will Industrie-Einsatzgruppe zur Jagd auf Cyber-Verbrecher

Wichtige Security-News, letzte drei Monate 2/2

- Kredit-Spam verzehnfacht in Q1
- Spammer beschicken ISPs nacheinander, um Blacklisten zu unterlaufen
- Polnischer Provider in Q1 größtes Zombienest (Brasilien zuvor)
- Große Koalition beschließt Selbstbeteiligung für Schäden von Managern
- Phishing frisierte Seiten am häufigsten aus Gesundheitsbereich

Top 10 Web Categories Manipulated by Phishing	
Rank	**Category**
1	Health & Medicine
2	Web-based Email
3	Finance
4	Computers & Technology
5	Chat
6	Search Engines & Portals
7	Social Networking
8	Personal Sites
9	Download Sites
10	Politics

Source: Commtouch Labs

BSI: Die Lage der IT-Sicherheit in D 2009

Gefährdungstrends

Bedrohung	2007	2009	Prognose
Zero Day Exploits	↑	↑	→
Drive-by-Downloads	—	↑	↑
Trojanische Pferde	↑	↑	↑
Viren	↓	↓	→
Würmer	↓	↓	→
Spyware	↑	↑	→
DDoS-Angriffe	→	↑	↑
Unerwünschte E-Mails	↑	↑	↑
Bot-Netze	→	↑	↑
Identitätsdiebstahl	↑	↑	↑
Betrügerische Webangebote	—	↑	→
Abstrahlung	—	→	→
Materielle Sicherheit, Irrtum, Nachlässigkeit	→	↑	→

↑ Gefährdung nimmt zu → gleichbleibende Gefährdung ↓ Gefährdung sinkt

BSI: Die Lage der IT-Sicherheit in D 2009

Risikoprofil innovativer Anwendungen und Technologien

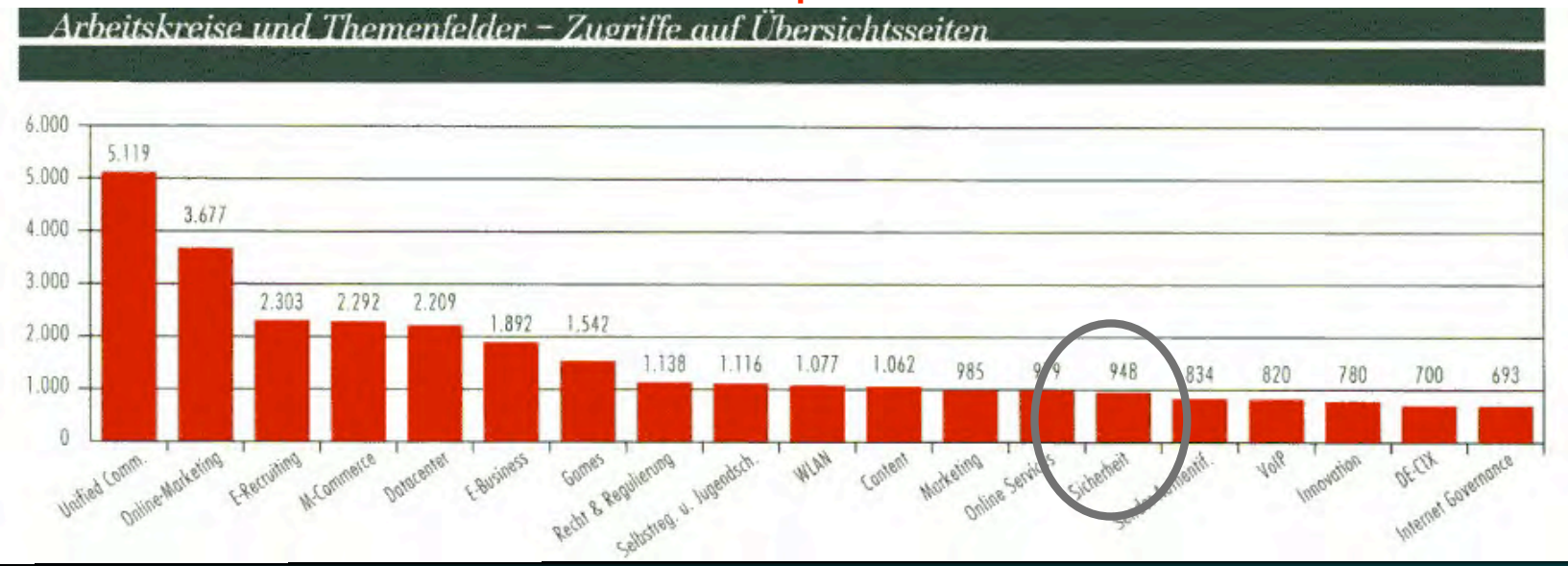
Technologie / Anwendung	2007	2009	Prognose
RFID	→	→	↑
Biometrie und Personaldokumente	—	↑	↑
IPv6	—	↑	→
Automotive	—	↑	↑
Gesundheitskarte	—	↑	→

↑ Gefährdung nimmt zu → gleichbleibende Gefährdung ↓ Gefährdung sinkt

In eigener Sache
Verschiedenes, Termine und Themen

- 3 Regeltermine pro Jahr: erster Mittwoch 02 / 05 / 10
  nächster also 07.10.09
  ggf. weitere Treffen nach Bedarf
- Thema am 07.10.2009
  ??? Themenpate gesucht
- **Bitte klicken!**

http://www.eco.de/arbeitskreise/sicherheit.htm



Gerne beantworte
ich Ihre Fragen

pallas

Dr. Kurt Brand
Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

information (at) pallas.de
http://www.pallas.de