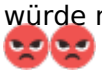
Erledigt Könnte so ko****** Ransomware in der Firma

Beitrag von „Sascha_77“ vom 27. Juni 2017, 17:01

Ich arbeite bei nem großen Konzern. Heute stürzte auf zig Rechnern Windows ab und ein angebliches chkdsk fand dann statt. Nur was das aber eine Ransomware die lustig die Platte verschlüsselte. Dann am Ende ein Reset und es gab einen schwarzen Schirm mit roter Schrift. .... Tja ..... Ende im Gelände.

Rechner in 3 Ländern betroffen (und die Zahl wird noch steigen). Ich habe bei uns den elektronischen Rechnungsempfang eingeführt habe und extra dafür einen Rechner gebastelt habe der von der Texterkennung bis hin zum Eingangsstempel und Ausdrucken alles vollautom. macht. Vor kurzem dann noch eine Dokumentenverwaltung eingerichtet da drauf. Es lief alles perfekt. Eine 2. SATA Platte als Spiegelung war ebenso vorhanden. Und noch ein Extra Plattenimage was ich auf meinem Arbeitsplatz Rechner gesichert habe.

ALLES weg. Ihr könnt euch nicht vorstellen wie ich kotzen könnte. Monate/Jahrelange Arbeit mit viel Schweiss und Blut (ich mache die Sachen dort neben meinem eigtl. Tätigkeitsfeld noch nebenher) .... WEG. Das der Konzern das Lösegeld zahlt halte ich für nicht wahrscheinlich. Da würde man von zig Millionen Dollar sprechen.


Ich bin gespannt was in den nächsten Tagen auf der Arbeit abgeht. Werde morgen erstmal ein Linux Laptop mitnehmen und gucken ob ich vllt. noch ein paar Scripte von der Spiegelplatte retten kann. Aber Hoffnung habe ich nciht wirklich.

Beitrag von „Doctor Plagiat“ vom 27. Juni 2017, 17:06

Schöne Sch....

Aber so ein großer Konzern hat doch bestimmt komplette Datensicherungen.

Beitrag von „Sascha_77“ vom 27. Juni 2017, 17:09

Naja ... wir haben bei uns im Standort einen eigenen Fileserver. Da steckt auch brav ein USB NAS als Backupmedium dran. Das wird alles futsch sein. Heisst es gibt für uns kein Backup mehr. Bin gespannt was mit SAP ist. Wenn die Datenbanken auch noch weg sein sollten dann gute Nacht. Aber die werden ja wohl auf ein Medium gesichert was man dann in den Schrank legt (hoffe ich doch mal).

Wir sind ein Tochterunternehmen dem Konzern zugehörig. Da rödeln jeweils eigene Server vor Ort mit lokalem Backup.

Beitrag von „al6042“ vom 27. Juni 2017, 17:10

Ach du Sch*****...
da bleibt mir fast die Spucke weg.

Beitrag von „Sascha_77“ vom 27. Juni 2017, 17:13

Ja und ich glaube wir sind nicht alleine. Gestern wollte ich ein Paket zur Post bringen in Düsseldorf. Kam zum Eingang ... hing ein Schild: Filiale wegen technischer Störung geschlossen. Die Packstation ging auch nicht mehr. Die werden wohl ein Tag vor uns Besuch von Mr. Ransom bekommen haben.

Beitrag von „derHackfan“ vom 27. Juni 2017, 17:15

Das sind Berufserfahrungen die kein Mensch braucht, ich drücke dir die Daumen ...

Beitrag von „Doctor Plagiat“ vom 27. Juni 2017, 17:16

> Zitat von Sascha_77
>
> Da steckt auch brav ein USB NAS als Backupmedium dran

Und wenn die Verzeichnisse gemappt sind bzw. im Netzwerk erreichbar, hat der Trojaner die auch verschlüsselt.

Beitrag von „mhaeuser“ vom 27. Juni 2017, 17:21

> Zitat von Sascha_77
>
> ALLES weg. Ihr könnt euch nicht vorstellen wie ich kotzen könnte. Monate/Jahrelange Arbeit mit viel Schweiss und Blut (ich mache die Sachen dort neben meinem eigtl. Tätigkeitsfeld noch nebenher) .... WEG. Das der Konzern das Lösegeld zahlt halte ich für nicht wahrscheinlich. Da würde man von zig Millionen Dollar sprechen.
> 

Versuch doch einfach herauszufinden, welche Ransomware das ist und such nach 'nem Decryption-Key bzw. revers' das Teil, um ihn zu "errechnen".

EDIT: Meh, steht ja sogar 'ne E-Mail-Adresse dabei... drei Sekunden gegooglet: Es ist eine neue Petya-Variante, wahrscheinlich funktioniert die Entschlüsselungsmethode für die alte auch noch (kann mir nicht vorstellen, dass mehr als die E-Mail-Adresse usw. geändert wurde).

Beitrag von „Wolfe“ vom 27. Juni 2017, 17:23

Wired schreibt dazu:http://www.wired.co.uk/article...attack-outbreak-june-2017

http://www.wired.co.uk/article...ck-outbreak-june-2017

Beitrag von „kuckkuck“ vom 27. Juni 2017, 17:23

> Zitat von Download-Fritz
>
> einfach

Das kann bei einer guten Verschlüsselung schön lange brauchen 

@Sascha_77 Ich drücke dir ebenfalls die Daumen!

Beitrag von „ralf.“ vom 27. Juni 2017, 17:24

Hab hier auch was - Ukraine. Sieht genauso aus
https://de.sputniknews.com/pan...7316347254-ukraine-virus/

Beitrag von „mhaeuser“ vom 27. Juni 2017, 17:29

> Zitat von kuckkuck
>
> Das kann bei einer guten Verschlüsselung schön lange brauchen 

Nö, die "Macht der Verschlüsselung" ist dahin, wenn man alle Infos für den Algo hat... in so einem Fall kann es ja gar nicht anders sein. Verschlüsselung ist nur sinnvoll, wenn der Masterkey nicht von bekannten Faktoren abhängt.

Beitrag von „Wolfe“ vom 27. Juni 2017, 17:34

Mit unwahrscheinlich viel Glück könnte das hier helfen:
https://www.heise.de/security/...oeffentlicht-3167064.html

Beitrag von „kuckkuck“ vom 27. Juni 2017, 17:35

@Download-Fritz Einen Versuch ist es sicherlich wert! Die Infos für den Algorithmus zu finden kann jedoch auch eine Challenge sein.

Beitrag von „Sascha_77“ vom 27. Juni 2017, 17:41

> Zitat von Wolfe
>
> Mit unwahrscheinlich viel Glück könnte das hier helfen:
> https://www.heise.de/security/...oeffentlicht-3167064.html

Das liest sich doch mal verdammt gut. Ich glaube ich nehme direkt noch ne Win7 DVD mit und setze mir ein system sauber neu auf und hänge die verseuchte Platte dran.

EDIT:
Zu früh gefreut. Der Generator ist nicht mehr da. 

Beitrag von „theo55“ vom 27. Juni 2017, 18:33

Ja auch bei einem "großen Konzern" (lol) sitzen viele Dilettanten die dann Mails öffnen, die man nicht öffnen sollte,
denn daher kann ja dieser Ransomware nur gekommen sein.

Also den Schuldigen suchen und bestrafen !!!

Beitrag von „Wolfe“ vom 27. Juni 2017, 18:40

Die Wahrscheinlichkeit, dass der Petya-Generator von 2016 heute erfolgreich angewendet werden kann, ist extrem gering. Ich dachte, ich tue mal etwas gegen Hilflosigkeit.

Der Angriff hat auf jeden Fall Nivea.

Beitrag von „Sascha_77“ vom 27. Juni 2017, 18:59

Wenn wirklich alle konzernweit verseucht sein sollten würde man von einem Lösegeld um die 60 Mio. Dollar sprechen. Bin echt schon auf morgen früh gespannt was es dann für Neuigkeiten gibt.

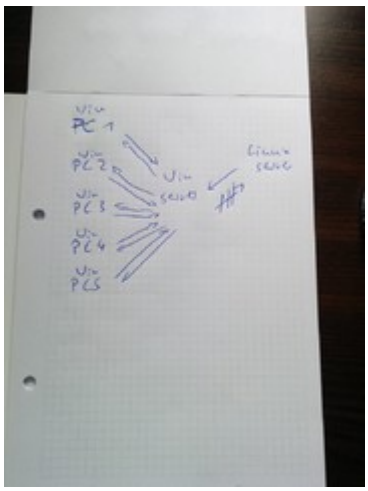
Beitrag von „Schorse“ vom 27. Juni 2017, 19:53

phuuu... mir ist ganz anders und das nur beim lesen

https://www.heise.de/security/...er-Angreifer-3757283.html

Beitrag von „Patricksworld“ vom 27. Juni 2017, 19:54

Kann nur nicht verstehen wie so ein großer Konzern so schlampig mit den Backups umgeht. Meine lösung in unserem 5 Mann Betrieb sieht ungefähr so aus.



Soll heißen. Die Windows PC's machen alle automatische Backups auf den WindowsServer PC. Auf den WindowsserverPC hat auch der Linuxserver zugriff. Allderings hat der WindowsPC keinen zugriff auf den Linuxserver. Und der linuxserver grabbt sich einfach immer die Backups vom Windowsserver. So ist mindest auf dem Linuxserver immer ein Funktionierendes Backup.

Beitrag von „Sascha_77“ vom 27. Juni 2017, 19:57

Tja in der Tat. So eine Linux-Lösung wäre eine gute Sache. Aber ich denke mal, dass nach diesem Vorfall sich wohl grundlegend was ändern wird. Möchte nicht wissen was da heute für ein Aufschrei durch gewisse Reihen gegangen ist. Einen größeren GAU als diesen gibts in der IT-Welt ja fast gar nicht.

Beitrag von „Schorse“ vom 27. Juni 2017, 20:05

Ist aber auch krass wie Microsoft mit kritischen Lücken umgeht..
A: Bekannte Lücke wie erneut von der NSA
b: Da wird die Hauseigene SercurLösung auf den WinKisten via update deaktiviert und das ohne Meldung an den Member.

Kopfschütteln...

Beitrag von „Raoul Duke“ vom 27. Juni 2017, 20:13

> Zitat von Schorse
>
> Ist aber auch krass wie Microsoft mit kritischen Lücken umgeht..

Oder die NSA, die die Lücke lieber selber nutzen wollte statt die Info an Microsoft weiterzugeben...

Beitrag von „Schorse“ vom 27. Juni 2017, 22:26

oder so

Wirklich wichtig ist natürlich WhatsApp Nachrichten mitzulesen, dadurch wird alles und jede angedachten KriminelleTat durchschaut.
"Ironie ende"

Sascha@ ich wünsche dir zeitnah eine Lösung, vielleicht ja sogar ein Hackcode zur Dechiffrierung. Du bekommst eine Daten zurück, dauert nur unter Umständen etwas. Habe Geduld..

Beitrag von „Saskia0201“ vom 27. Juni 2017, 23:23

krass echt krass, wünsche dir das beste. Das wünscht man selbstdem schlimmsten feind nicht...

Beitrag von „Sascha_77“ vom 28. Juni 2017, 08:44

Danke Leute für die "Anteilnahme".

Da sind wir mit erwähnt:

http://www.focus.de/digital/rueckkehr-von-wannacry-hacker-greifen-firmen-in-europa-an_id_7290825.html

@Schorse
Genau so ist es. Die Prioritätenverteilung in unserem Land ist arg fragwürdig.

EDIT:
Mein Chef rief grad an uns meinte ich soll zu Hause bleiben. Aber angeblich hätte die IT erste Lösungen erarbeitet. Man darf gespannt sein.

Beitrag von „umax1980“ vom 28. Juni 2017, 10:10

Gab / Gibt es keine Backupstrategie die jetzt einspringen könnte ??
Finde ich bei einem Unternehmen einer gewissen Größe schon eine wichtige Frage ....

Beitrag von „Sascha_77“ vom 28. Juni 2017, 10:33

Wie gesagt ... die einzelnen Standorte haben jeweils einen eigenen Server mit Backup. Konzernweit wird das nicht Zentral abgelegt.

Wir hatten früher mal eine Sicherung auf Band. Als der Streamer dann kaputtging gabs ein USB Storage als Backuplösung. In so einem Fall wie jetzt natürlich denkbar ungünstig. Einfach eine

kleine Linuxkiste wäre da als Backupmedium besser gewesen.

Wie schonmal gesagt. Ich denke jetzt wird ein Umdenken stattfinden und Maßnahmen ergriffen, dass sowas so nicht noch mal eintreten kann. Bzw. das man sich eine Ransomware einfängt kann man nie ausschließen aber das zumindest Backuptechnisch alles in trockenen Tüchern ist.

Beitrag von „umax1980“ vom 28. Juni 2017, 10:57

Hoffentlich ist ein Backup greifbar, wenn auch ein paar Tage alt.

Beitrag von „Sascha_77“ vom 28. Juni 2017, 11:11

Man wirds sehen. Ich hatte zwar die USB Platte einfach abgezogen aber vllt. war es da schon zu spät.

Beitrag von „LuckyOldMan“ vom 28. Juni 2017, 11:22

> Zitat von Sascha_77
>
> ....
> Wir hatten früher mal eine Sicherung auf Band. Als der Streamer dann kaputtging gabs ein USB Storage als Backuplösung. ...

Ja die ollen Streamer mit ihrem Großvater/Vater/Sohn-Prinzip. Hatte wir in den 90ern auch so eingerichtet. So schlecht war das nicht.

Beitrag von „Sascha_77“ vom 28. Juni 2017, 11:32

Irgendwie schon.

Habe jetzt gerade einen internen Link bekommen um den Status schauen zu können. Die schwärmen jetzt in die Standorte aus um die Rechner die nicht betroffen sind mit nem Script zu schützen.

Von der Entschlüsselung steht da noch nix. Aber klar das das nicht von jetzt auf gleich geht (wenn überhaupt).

Beitrag von „Rasselkopp“ vom 28. Juni 2017, 11:53

Was habt ihr den für eine Windoof Version auf den Rechner da bitte? XP noch?

Es soll ja eine Malware sein und die fällt ja auch nicht so einfach vom Himmel.
Aber lass mal ich war letztens beim Schwager im Büro der lief der Rechner der Tippse nicht richtig, brauchte ehwig zum hochfdahren und war dan kaum benutzbar.
Der war voll ausgelastet, also PLate raus an Laptop ran und nur mal ADWCleaner laufen lassen.
2900 Schadenssoftware EInträge, also Regestrierung, Startdateien, Tollbars und das beste 2 BitcoinMainer.
Selbst bei den Disponenten waren Hunderte EInträge.
ALs Antwort kam dann," ich war das nicht", "ich hab das nicht installiert oder runter geleladen"

Hier waren die Leut aber selber Schuld. Windows XP noch ohne Sicherheitssoftware und nix mit Backup.
Der Hauptgrund ist gewesen ,das eben mal schnell was runterladen und im empfolen Modus installieren mit Drittanbieter Software dazu oder Mailanhäge öffnen
bei denen eine EXE dahinter steht.
Jetzt rödelt da Win7 auf alle Rechner mit Symantec Endpoint, ein NAS als Backup und Aminrechte haben die keine mehr.
Nur noch an und Ausschalten dürfen sie. nicht mal Updates installieren.
Aber wenn du 10 Rechner hast und 9 Bombensicher sind kann der letzte durch Unachtsamkeit

alles lahm legen.
L.G.

Beitrag von „Sascha_77“ vom 28. Juni 2017, 11:56

Bei uns ist Win7 in Betrieb. Wird langsam alles auf 10 umgestellt.

Beitrag von „Rasselkopp“ vom 28. Juni 2017, 12:00

Na wer weiß wo ihr euch das eingefangen habt.

Ich halte ja nichts von kostenlosen Tools aber adwcleaner kann man ab und zu laufen lassen. Gerade in Büros wo einige ihre privaten Dinge und Downloads erledigen hat das schon geholfen.

Gesendet von iPad mit Tapatalk

Beitrag von „Sascha_77“ vom 28. Juni 2017, 12:29

Der Inet Verkehr läuft über nen Proxy. Da ist ne dicke Blacklist drin. Man kann viele Seiten gar nicht erst aufrufen. Aber gut ... kommt jemand mit nem USB Stick daher kanns das dann u.U. auch gewesen sein.

Beitrag von „umax1980“ vom 28. Juni 2017, 12:51

Gastnutzer ist sowieso Pflicht bei uns, da kann schon mal keiner als was anderes arbeiten.
Momentan ist auf allen Rechnern bei uns Windows 7 installiert.

Gesichert wird täglich auf ein NAS, soweit ich das weiss, stehen aber an verschiedenen Standorten und
kennen sich untereinander nicht, es wird auch immer auf ein anderes NAS gesichert, sodaß im schlimmsten
Fall die Daten von 2 Tagen weg sind.

Aber unser Admin ist ein Sicherheits-Fanatiker. Ich finde, man kann es auch übertreiben. Den Nutzern
erklären, wie sowas passieren kann und was man tun und lassen sollte. Das wäre viel wichtiger..

Beitrag von „Sascha_77“ vom 28. Juni 2017, 13:05

Genau ... weil Fakt ist, dass der menschliche Faktor der größte von allen in so einer Sache ist.

Beitrag von „jboeren“ vom 28. Juni 2017, 13:07

Ich drück dir/euch die Daumen @Sascha_77! Was für eine sch**ss geschicht....

Da hört sich mein kaputter kühlschrank als kleinkram an....

Beitrag von „KayKun“ vom 28. Juni 2017, 16:11

Du hast mein Mitleid ich durfte das gleiche gestern bei einen freund, der ein Restorang hat,

machen zum Glück nur ein Back Office Laptop eine Windows Kasse und ein Windows Server.

Zum Glück hatte ich vor kurzen dort ein RPI mit einer Externen HDD als Backup gemacht die nur zugriff auf den Server hatte und nur Daten von da sich geholt hatte sonst wahr kein zugriff zum PI hin.

Gestern 4 Stunden alles Neu installiert + Super leckeres kostenfreies Essen bekommen und alles wahr wieder in Ordnung.

Beitrag von „theo55“ vom 28. Juni 2017, 17:09

@Rasselkopp . jawohl Du sagst es genau richtig, wenn man schon Windoof einsetzt (und welch ein Wunder... in einem "großen Konzern" - ist wohl eher ne kleine Kramsbude !)
läuft dann noch Win7. Nicht mal auf Win8.1 hat es der "große Sch****-Konzern" geschafft upzudaten !
Ganz richtig das da mal sowas passiert, Dummheit (der Mitarbeiter) muss bestraft werden !!

Beitrag von „umax1980“ vom 28. Juni 2017, 17:21

Das kommt natürlich in einer gewissen Betrachtungsweise in Frage, aber es muss natürlich gewährleistet werden, daß sämtliche Programme die genutzt werden auch einwandfrei funktionieren.

Aber der Mensch ist der Unsicherheits-Faktor, das stimmt 100%...

Beitrag von „Raoul Duke“ vom 28. Juni 2017, 17:32

Es steht noch garnicht fest wie die ransomware in die Firmennetzwerke kam aber das sie sich

innerhalb der Netzwerke auch auf Windowrechnern die up-to-date sind ausgebreitet hat.

zu dem großen-Kramsbuden-scheiz sag ich mal nichts 

Edit:

> Zitat von Sascha_77
>
> Ich hatte zwar die USB Platte einfach abgezogen aber vllt. war es da schon zu spät.

encrypts ON BOOT. If you see CHKDSK message your files not yet encrypted, power off immediately. You can recover with with LiveCD

Beitrag von „Schorse“ vom 28. Juni 2017, 18:43

So sieht es wohl aktuell aus

http://www.zdnet.de/88302721/p...dium=rss&utm_campaign=rss

Beitrag von „mhaeuser“ vom 28. Juni 2017, 23:52

Da hab' ich mich wohl leider geirrt, sorry...
http://thehackernews.com/2017/...omware-wiper-malware.html

Beitrag von „Sascha_77“ vom 29. Juni 2017, 06:42

What?? Ich brech ins Essen. 

Beitrag von „McRudolfo“ vom 29. Juni 2017, 07:08

> Zitat
>
> Microsoft weist darauf hin, dass die zugrundeliegenden Schwachstellen am 14. März durch das Sicherheitsupdate MS17-010 behoben wurden.

Kein Kommentar....

Beitrag von „Sascha_77“ vom 29. Juni 2017, 07:28

Und dabei kriegen wir andauernd updates das es fast schon nervt. Sieht dann wohl nach Schlamperei aus.

Beitrag von „Sascha_77“ vom 29. Juni 2017, 09:30

Ich fress nen Besen Leute. Habe die Usb Platte vom Fileserver und die von dem Rechner fuer die Eingangsrechnung-Verarbeitung an das Debian Laptop gepackt .... Files da!!!! Jetzt zieh ich erstmal alle daten auf ne saubere usb platte.

Rettung in Progress.

Beitrag von „umax1980“ vom 29. Juni 2017, 09:48

"Schwein" gehabt.

Aber was sage ich immer: BACKUP RULEZ !!!

Beitrag von „KayKun“ vom 29. Juni 2017, 10:08

Nice da hast du ja richtig glück gehabt

Beitrag von „Sascha_77“ vom 29. Juni 2017, 10:27

Ja scheinbar befällt diese Variante von Petya "nur" das Systemvolume.

Beitrag von „Altemirabelle“ vom 29. Juni 2017, 10:27

Ich weiss es nicht ob es hier erwähnt wurde, aber für die die noch nicht infiziert sind gibt es angeblich eine einfache Medizin:
How to Enable the NotPetya/Petna/Petya Vaccine >> https://www.bleepingcomputer.c...etya-ransomware-outbreak/

Beitrag von „Sascha_77“ vom 29. Juni 2017, 10:32

Die Scripte werden bei uns bereits ausgerollt.

Beitrag von „Altemirabelle“ vom 29. Juni 2017, 11:46

@Sascha_77

Kannst du mal vermuten wie es zu der Infektion kam?

Beitrag von „Sascha_77“ vom 30. Juni 2017, 13:20

Kein Plan. Ich hab noch nix von der IT erfahren.

Keines der Patch-Scripte hat funktioniert hier im Standort. 

EDIT:
So die Patchscripte haben jetzt funktioniert. Die hatten das falsche Admin-Passwort im Script hinterlegt. 
7 Rechner konnte ich jetzt patchen. Der Fileserver blieb übrigens komplett unberührt wie sich heute rausstellte. Und mein Rechnungs-Rechner läuft nach Clonen des Spiegels nun auch wieder wie vorher.

Angeblich soll es eine 2. Welle gegeben haben. Aber wir hatten ja schon überall alles offline, sodass da nix passiert ist.

Es bleibt weiterhin spannend. Die infizierten Rechner werden nicht neu installiert sondern wir kriegen komplett neue. Denke da ist direkt Win 10 drauf da die Pilotphase dafür schon jetzt ein paar Monate her ist. Da ja ein paar tausend Geräte benötig werden kann man gespannt sein wieviel Lenovo auf Lager hat.  Und dann müssen die ja auch noch vom Helpdesk bespielt werden. Das kann was werden.

Beitrag von „Dr.Stein“ vom 30. Juni 2017, 13:22

Kommt die Versicherung für neue Rechner auf?
Was sind den das für neue Geräte? Ist ja echt mies so eine Attacke...

Beitrag von „Sascha_77“ vom 30. Juni 2017, 13:26

Seit 2017 leasen wir die Teile. Davor musste wir die kaufen. Weiss nicht wer für was aufkommt.

SInd die hier:
http://www3.lenovo.com/de/de/d...e-M900-Tiny/p/11TC1MTM900

Ziemlich coole Teile. Ich habe so einen schon länger da stehen bzw. eher liegen. 

Beitrag von „Dr.Stein“ vom 30. Juni 2017, 13:28

Die kleinen Geräte sind aber hübsch!
Klein und Leistungsstark... bestimmt auch was für MacOS X. 

Beitrag von „Sascha_77“ vom 30. Juni 2017, 13:30

Ja. Glaub meiner hat ne HD510 oder 520. Da müsste eigtl. was gehen.