Erpresserviren

Jupp Joachimski
Datenschutzbeauftragter der bayerischen (Erz-) Diözesen

Ein Computervirus

- ist ein
  - typischerweise in Maschinensprache geschriebenes
  - und als solches häufig nicht erkennbares
  - Computerprogramm,
  - das dem Verbreiter Vorteile – ggfs. auch nur ideeller Art – bringen soll und
  - den Computer, auf dem es sich installiert, in seiner Funktionsfähigkeit beeinträchtigt.
- Computerviren gibt es, seit es Software gibt.
- Ihre Zahl ist mit der Bedeutung des Internets gewachsen.
- Täglich kommen 60.000 Viren hinzu!

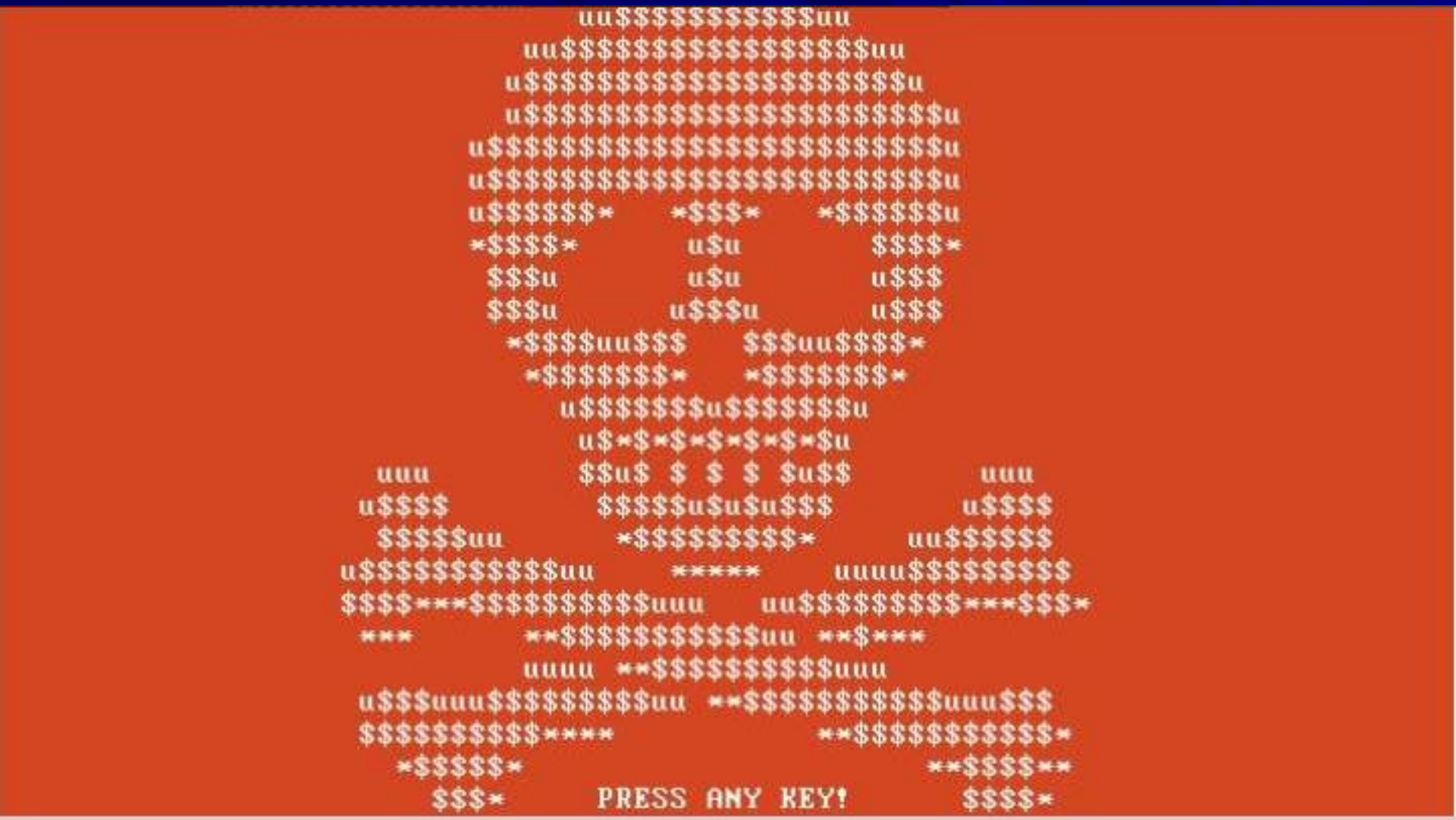
Die typischen Ziele von Computerviren

- Reine Störung der Funktionsfähigkeit der IT
  - aus bloßer Freude am Zerstören oder
  - zur Beeinträchtigung z.B. der Konkurrenz
- Gewinnung von Informationen aus dem infizierten PC
  - Kontakte
  - Geldwerte Informationen, z.B. Kontonummer
  - Geheimzahlen (Passwort, PIN)
- Beherrschung des fremden PC z.B. für
  - E-Mail-Versand von anderen Rechnern oder
  - Zugriffsattacken
- Erpressung von Vermögenswerten

Erpresser Virus Typ 1: **Desktop-Locker**

sperren den Zugang zu Windows und zeigen stattdessen eine erpresserische Nachricht an. Darin steht, wie das Opfer das Lösegeld bezahlen soll. Viren dieser Art gibt es bereits seit vielen Jahren. Sie versuchen oft, den Druck auf das Opfer zu erhöhen, indem sie vorgeben, vom Bundeskriminalamt (BKA) zu stammen. In der Nachricht behaupten sie, illegale Dateien auf dem PC gefunden zu haben. Varianten dieser Schädlinge geben vor, von Microsoft zu stammen und auch, illegal genutzte Software festgestellt zu haben. Desktop-Locker sind inzwischen seltener geworden und relativ einfach zu entfernen.

Typische Anzeige auf dem Monitor



BUNDESPOLIZEI

Es ist die ungesetzliche Tätigkeit enthüllt!

Achtung!!!

Ein Vorgang illegaler Aktivitaten wurde erkannt.
Das Betriebssystem wurde im Zusammenhang mit Versto?en gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Verto? festegestellt: Ihre IP Adresse lautet mit dieser IP wurden Seiten mit pornografischen Inhalten,Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen
Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten,Elementen von Gewalt und Kinderpornografie festgestellt! Es wurden auch Emails in Form von Spam,mit terroristischen Hintergrunden, verschickt. Diese Sperre des Computers dient dazu, Ihre illegalen Aktivitaten zu unterbinden.

Ihre Angaben: IP: Browser: OS: Windows Country: City: - ISP:

Um die Sperre des Computers aufzuheben, sind Sie dazu verflichtet eine Strafe von 100 Euro zu zahlen.Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.
1) Die Zahlung per Ukash begleichen:
Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK)
Sollte das System Fehler melden,so müssen Sie den Code per Email (einzahlung@landes-kriminalt.net) versenden.
2) Die Zahlung per Paysafecard begleichen:
Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK) Sollte das System Fehler melden,so müssen Sie den Code per Email(einzahlung@landes-kriminalt.net) versenden.

Ukash Ok

Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse).Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können

Tankstellen - jetzt auch erhältlich bei folgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.

epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

paysafecard
pay cash. pay safe.

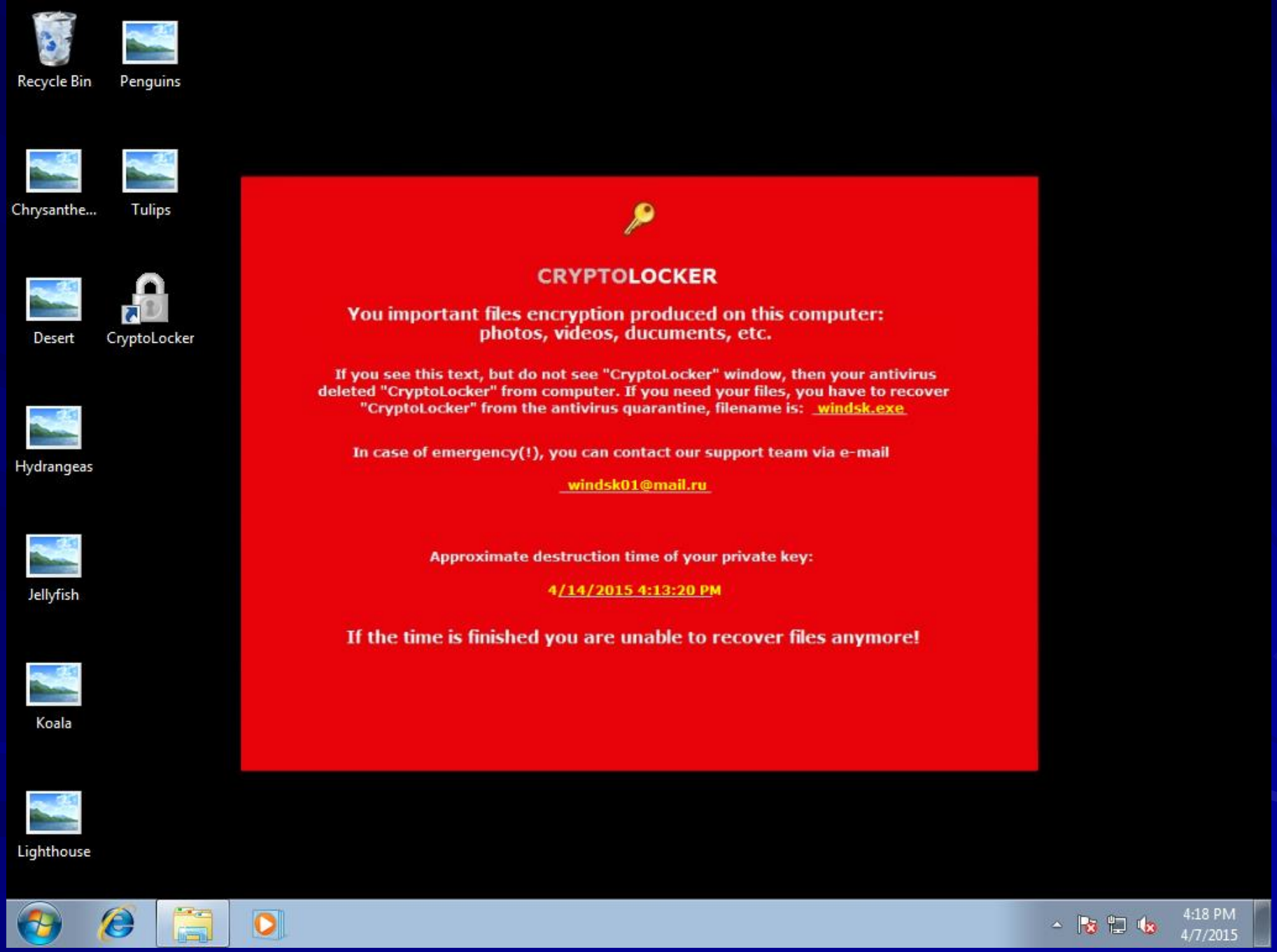
Ok

Erpresser Virus Typ 2: **Verschlüsselungs-Trojaner**

fordern ebenfalls ein Lösegeld. Als Zahlungsmittel sind meist Bitcoins oder Paysafe-Karten vorgesehen, da so der Empfänger anonym bleiben kann.

Im Gegensatz zum Typ 1 verschlüsseln sie aber Dateien und zwar meist abhängig vom Dateityp, z.B. alle Dateien mit den Endungen .jpg, .docx und .xlsx. Da es sich um Anwenderdateien handelt, benötigt der Virus keine besonderen Zugriffsrechte. Neuere Varianten versperren auch den Zugang zur kompletten Festplatte.


Your personal files are encrypted by CTB-Locker.
Ihre persönlichen Dateien sind von CTB-Locker verschlüsselt.
Ihre Dokumente, Fotos, Datenbanken und andere wichtige Dateien mit stärkste Verschlüsselung und eindeutigen Schlüssel, die für diesen Computer generiert verschlüsselt wurden.
Privatentschlüsselungsschlüssel ist auf eine geheime Internet-Server gespeichert und niemand kann Ihre Dateien zu entschlüsseln, bis Sie zahlen und die privaten Schlüssel erhalten.
Sie haben nur 96 Stunden, die Zahlung zu einreichen. Wenn Sie Geld im vorgesehenen Zeit nicht senden werden alle Ihre Dateien permanent verschlüsselt bleiben und niemand wird in der Lage sie wiederherzustellen.
Drücken Sie 'Ansicht', um die Liste der Dateien, die verschlüsselt wurden ansehen.
Drücken Sie auf 'Weiter' für die nächste Seite.
WARNUNG! VERSUCHEN SIE NICHT UM DAS PROGRAMM SELBST LOSZUWERDEN. ALLE MAßNAHME WIRD ENTSCHLüSSELUNGSSCHLüSSEL FÜHREN ZERSTöRT. SIE WERDEN IHRE DATEIEN FüR IMMER WERLIEREN. NUR SO ZU HALTEN IHRE DATEIEN IST DIE ANWEISUNG ZU FOLGEN.
Ansicht
95:14:16
Weiter >>


Recycle Bin
Penguins
Chrysanthe...
Tulips
Desert
CryptoLocker
Hydrangeas
Jellyfish
Koala
Lighthouse
CRYPTOLOCKER
You important files encryption produced on this computer:
photos, videos, ducuments, etc.
If you see this text, but do not see "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer. If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, filename is: windsk.exe
In case of emergency(!), you can contact our support team via e-mail
windsk01@mail.ru
Approximate destruction time of your private key:
4/14/2015 4:13:20 PM
If the time is finished you are unable to recover files anymore!
4:18 PM
4/7/2015

In the case of payment of a fine, all data collected against you will be removed from the evidence base

First violations committed not entail any legal consequences, except a penalty in accordance with the law of February 18, 2013. For repeated violation of the law prosecution is inevitable.

Incorrect payment code

green dot MoneyPak

MoneyPak is available at these stores nationwide: Walmart, Kroger, CVS/pharmacy, Kmart, Rite AID pharmacy, Meijer, Ralphs, Walgreens, FredMeyer, Eleven, Food4Less, Fry's, WinnDixie and etc.

Exchange cash for a MoneyPak voucher and enter the voucher code in the form below

Code: Submit

1 2 3 4 5 6 7 8 9 0

OR

paysafecard

You can get Paysafecard at Epay, from King Kullen supermarket, Tom Thumb, PayXChange, Randalls, ShopRite, Precash, SafeWay, Genuardi's, PriceRite, Dominick's.

Exchange cash for Paysafecard voucher and enter the voucher code in the form below

Code: Submit

1 2 3 4 5 6 7 8 9 0

Please note: Penalties can be paid within 48 hours. If the fine is not paid within this period, you can not unlock the computer. In this case against you will be prosecuted.

Where can I buy MoneyPak?

Walmart · 7-Eleven · RITE AID PHARMACY · kmart · Walgreens · CVS/pharmacy

Where can I buy Paysafecard?

epay · SAFEWAY · ShopRite · PRECASH · Dominick's Ingredients for life.. · GENUARDIS · PRICE RITE

Wie erfolgt die Infektion?

Erpresserviren kommen hauptsächlich über spamartig verbreitete Mails, meist sehr gut gemachte Trickmails. Das Aussehen der Mails wirkt echt, die Nachricht scheint plausibel, und der Anhang ist meist ein harmlos wirkendes PDF oder eine Word-Datei. So öffnen die Empfänger der Nachricht häufig das angehängte Dokument. In der Datei befinden sich aber gefährliche Codeteile, die Sicherheitslücken von Word oder dem Acrobat Reader ausnutzen und im nächsten Schritt weiteren Code, meist den eigentlichen Verschlüsselungstrojaner, aus dem Internet nachladen und gleich starten.

Typische Betreffzeilen

- Your Apple account has been closed.
- Sie haben folgende Pay-Pal-Zahlung geleistet.
- Rechnung der Fa. XXXX
- DHL-Paket-Lieferung fehlgeschlagen
- Sie haben gewonnen
- Ihr Konto wird gesperrt
- Abmahnung
- Lieferschein
- Forderung

Andere Infektionswege

- Die neuesten Generationen der Ransomware kommen ganz ohne Anhänge aus und verwenden direkt in die E-Mail eingebettete JavaScripts, welche viel schwieriger zu erkennen sind und meist nur als „Erstinfektor“ (Dropper) fungieren, um die eigentliche Malware nachzuladen.
- Dass Erpresserviren durch das bloße Aufsuchen einer Webseite auf den Rechner gelangen können, wird zwar immer wieder einmal berichtet, doch konnte es nicht nachvollzogen werden.

Was wird infiziert?

- Alle Windows-Versionen von XP bis Windows 10
- Mittlerweile sind auch schon in beachtlichem Umfang Dienstrechner öffentlicher Behörden betroffen, z. B. Dettelbach und Zürich.
- Android-Tablets und –Smartphones. Allerdings sind die Viren relativ einfach von diesen Geräten zu entfernen (vgl. später).
- Apple-IPhone und –Tablets: Keranger-Virus

Wie verhindert man eine Infektion?

- Die größte Schwachstelle des Computers ist die Person, die vor dem Monitor hockt.
- Sie reagiert im wahrsten Sinne des Wortes menschlich mit Neugier, Unwissenheit und irrationalen Ängsten.
- Diese Mischung nutzen die Kriminellen.
- Wenn man sich darüber erst einmal klar ist, hat man schon die halbe Gefahr beseitigt.
- Jetzt kommt es darauf an, planvoll vorzugehen, um die Risiken zu minimieren.
- Zum Beispiel beim Eingang eines E-Mails:

Der Rat des BSI

Alle Sicherheitsmaßnahmen zur Kontrolle

- Installieren und aktualisieren Sie AntiViren-Software, Anti-Trojaner-Software, SPAM-Filter, Firewall und IPS so oft wie möglich.
- Konfigurieren Sie SPAM-/Viren-Filter so, dass JavaScript-Inhalte von nicht vertraulichen Quellen geblockt werden.
- Hindern Sie, wenn möglich, JavaScript am automatischen Ausführen (direkt im SPAM-Filter oder am Mailserver bzw. im E-Mail-Programm).
- Löschen Sie Mails mit Links und Anhängen nicht bekannter Absender bzw. nicht erwartete Nachrichten im Zweifelsfall.
- Halten Sie Betriebssysteme, Webbrowser, Java, Flash immer auf dem neusten Stand.
- Flash und Java sollten im Browser besser grundsätzlich abgeschaltet sein. Bei Firefox: Menü – Extras – Addins – Plugins – Shockwave.Flash bzw. Java: *Nachfragen, ob aktiviert werden soll*.
- Aktivieren Sie in Windows die Anzeige der bekannten Dateitypen.
- Deaktivieren Sie Makros oder verwenden Sie nur entsprechend signierte Makros.
- Informieren Sie sich und Ihre Mitarbeiter über die aktuellen Gefahren.

Die beste Sicherung gegen Erpressung

- Legen Sie aktuelle Backups aller für Sie wichtigen Dateien auf externen Speichermedien an, aber schalten Sie diese im Normalbetrieb ab!
- Es ist wichtig, dass das Backupprogramm in regelmäßigen Abständen die Änderungen abspeichern kann, ohne den gesamten Speichervorgang wiederholen zu müssen; sog. „differenzielle Sicherung“.
- Gute (und kostenfreie) Backup-Lösung, die alle Anforderungen erfüllen kann:
  http://personal-backup.rathlev-home.de/

Und wenn doch etwas passiert ist:

- Einige Antivirenhersteller arbeiten laufend daran, neue Entschlüsselungstools bereitzustellen. So brachte Eset ein Entschlüsselungstool für Teslacrypt-Opfer (Version 3 bis 4.2) heraus. Kaspersky bietet Decrypter gegen einige Erpresserviren, Emsisoft Entschlüsselungstools für zahlreiche Erpresserviren.
- Sicherheitsexperten empfehlen in der Regel, das Lösegeld nicht zu zahlen. Denn keiner kann sich darauf verlassen, dass er nach der Zahlung einen funktionierenden Code zum Entschlüsseln oder Entsperren erhalten. Außerdem würde man mit einer Zahlung die Kriminellen dazu ermutigen, weiter Schädlinge zu verbreiten und indirekt die Entwicklung weiterer Erpresserviren bezahlen. Trotzdem gibt es in der Praxis immer wieder auch erfolgreiche Zahlungen.
- Jedenfalls ist es sinnvoll, die verschlüsselten Daten zu speichern, weil oft erst nach einiger Zeit ein Schlüssel gefunden und veröffentlicht wird.

So entfernen Sie Erpresser-Viren von Android-Geräten

Nutzen Sie ein Handy mit Android ab **Version 4.1**, dann versuchen Sie, Ihr Smartphone im **abgesicherten Modus** zu starten. Android bootet so nur mit einer minimalen Konfiguration, was die Ausführung der Schad-Software verhindert. So haben Sie die Möglichkeit, den Virus über die **Einstellungs-App** zu **deinstallieren**.

In den abgesicherten Modus kommen Sie über eine Taste oder Tastenkombination. Diese unterschiedet sich allerdings nicht nur von Hersteller zu Hersteller, sondern teilweise auch von Modell zu Modell.

Fast alle **Geräte** müssen Sie **zuerst ausschalten**. Sollte das der **Erpresservirus verhindern, entfernen Sie kurz die Batterie**. Geht das nicht, müssen Sie warten, bis diese leer ist.