POLIZEI
Nordrhein-Westfalen
Düsseldorf

bürgerorientiert · professionell · rechtsstaatlich

Polizeipräsidium Düsseldorf · Kommissariat Kriminalprävention/Opferschutz

Präventionshinweise für Bürgerinnen und Bürger
Ausgabe 6

„Steigende Fallzahlen im Bereich Ransomware/Kryptotrojaner“

Vorwort

Liebe Düsseldorferinnen und Düsseldorfer,

immer häufiger verschaffen sich Kriminelle mit zum Teil einfachsten Mitteln Zugriff auf den Rechner und sperren diesen für den eigentlichen Nutzer oder verschlüsseln die Dateien. Der Betroffene soll in der Folge die Freigabe mit einem „Lösegeld“ erkaufen.

Die Täter greifen nicht nur Firmencomputer an, sondern auch die Rechner von Privatleuten, die ihre Fotos, Unterlagen etc. gespeichert haben. Leider nehmen diese Attacken auf die Computer immer mehr zu. Wie Sie sich vor solchen Verschlüsselungstrojanern oder auch Ransomware besser schützen können, erläutern wir Ihnen auf den nächsten Seiten.

Susanna Heusgen,
Leiterin der Kriminalprävention

Ransomware/Kryptotrojaner

Ein Befall der EDV-Infrastruktur mit einem Verschlüsselungs-Trojaner („Ransomware“) kann jeden treffen:

Privatpersonen, Einzelhändler, mittelständische Unternehmen oder große Klinikbetriebe. Der dabei entstehende Schaden ist meist beträchtlich.

Ohne Zugriff auf ihre Daten können viele Unternehmen nicht arbeiten, Patienten nicht versorgt werden, Waren nicht ausgeliefert werden, oder kritische Dienstleistungen wie Energie- oder Wasserversorgung nicht erbracht werden.

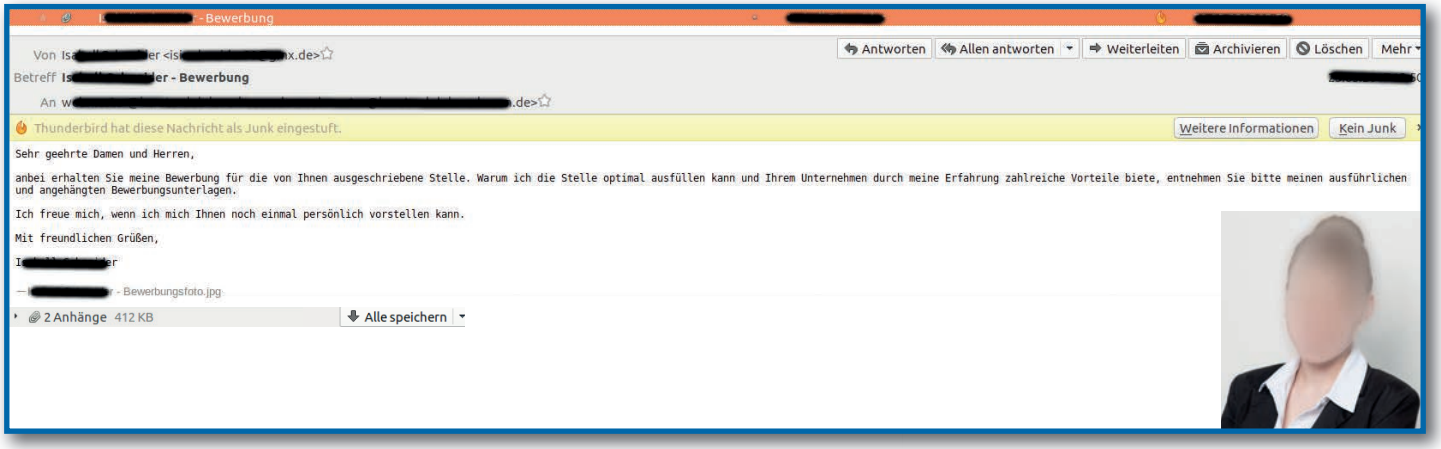
Auch für Privatpersonen kann ein Verschlüsselungstrojaner üble Folgen haben, wenn zum Beispiel das Online-Banking mit ausspioniert wurde, oder der Datenbestand eines ehrenamtlich geführten Vereins nicht mehr zugänglich ist. Aber auch ein emotionaler Schaden, wenn beispielsweise Bilddateien mit Fotos der Enkelkinder verschlüsselt wurden, kann für Privatpersonen beträchtlich sein.

POLIZEI
Nordrhein-Westfalen
Düsseldorf

Was passiert?

Auf dem Computer wird eine Schadsoftware ausgeführt, welche die Daten auf allen erreichbaren Datenträgern, auf die der jeweilige Benutzer Zugriff hat, verschlüsselt. Das können Laufwerke im Computer selbst sein, extern angeschlossene Speichersticks oder USB-Festplatten, aber auch eingebundene Netzwerklaufwerke auf Server- oder Cloudsystemen.
Diese Dateien sind dann nicht mehr mit den dazu vorgesehenen Programmen zu öffnen.

Danach bekommt der Anwender eine Aufforderung, einen Geldbetrag zu überweisen, um so an ein Entschlüsselungsprogramm zu gelangen. Die Geldzahlungen sollen meist in Form einer Kryptowährung erfolgen. Die Höhe des Betrages variiert und ist meist an das Opfer angepasst. Von Einzelpersonen können beispielsweise um die 1000 Euro gefordert werden, bei Industrieunternehmen jedoch durchaus Summen im Bereich von Hunderttausenden oder gar Millionen.



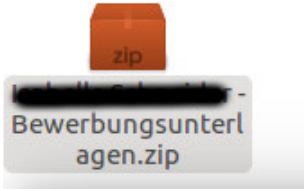
Ransomware/Kryptotrojaner

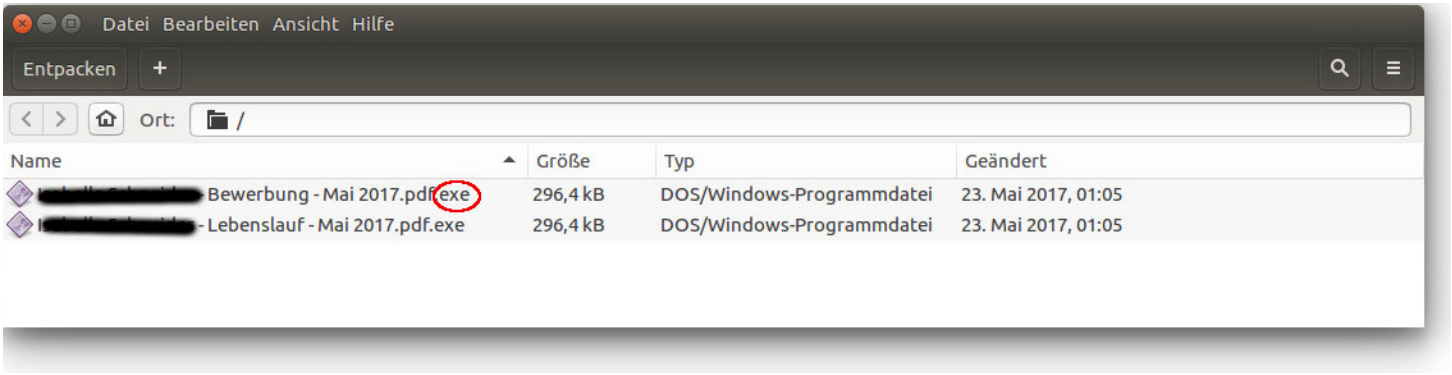
Wie gelangt Schadsoftware auf den Computer?

Der Haupteinfallsweg für Ransomware ist immer noch ein **unbedachter Klick auf einen Anhang** in einer E-Mail.

Allerdings nehmen auch andere Angriffsvektoren zu, beispielsweise über Sicherheitslücken in Betriebssystemen oder Anwendungsprogrammen, manipulierte Werbebanner bzw. „drive-by-Downloads“ (unbewusstes/unbeabsichtigtes Herunterladen von Schadsoftware allein durch Aufruf einer gezielt manipulierten Webseite) oder auch über manipulierte/gefundene USB-Sticks.

POLIZEI
Nordrhein-Westfalen
Düsseldorf





Vorbeugung & Vorsorge:

Zur Vorbeugung gegen Angriffe mit Ransomware gehört sowohl für Privatanwender als auch für Firmen vor allem die Beachtung von drei Punkten:

- Updates für Betriebssysteme und Anwendungsprogramme müssen aktuell sein.
  Verwenden Sie einen Virenscanner mit aktuellen Signaturen.
- Größte Vorsicht bei E-Mails mit Anhängen. Wenn beim Öffnen der Anhänge gesonderte Berechtigungen, z.B. zur Ausführung von Makros oder Programmen, erfragt werden: **Finger weg!**
- Es muss regelmäßig eine Datensicherung aller wichtigen Daten (z.B. Dokumente oder Bilder) auf unterschiedliche, externe Datenträger (z.B. USB-Sticks oder Festplatten) erfolgen. Sicherungsdatenträger dürfen niemals ständig mit dem Computer verbunden sein.

Ransomware/Kryptotrojaner

Das Schadpotential von Ransomware beruht aber nicht nur auf dem unmittelbaren Schaden, sondern auch darauf, dass viele Privatpersonen, Selbstständige oder Firmen auf den Ernstfall nicht vorbereitet sind. Sie sind der Meinung, dass es ausreicht, nicht Opfer einer solchen Attacke zu werden. Das ist aber nur dann ausreichend, wenn der Schutz zu 100 % funktioniert. Da es jedoch eine 100 %ige Sicherheit nie geben kann, muss man sich Gedanken machen, was im Falle eines Angriffs zu tun ist.

Die folgende Auflistung richtet sich vor allem an Firmen, kann aber teilweise auch von Privatpersonen umgesetzt werden. Sie ist aber nur als Anregung zu verstehen und kann keinesfalls eine sorgfältige Analyse ersetzen.

- Richten Sie eine E-Mail-Filterung ein, ggf. schon auf dem eigenen Mailserver, falls vorhanden.
- Schulen Sie Ihre Mitarbeiter in Bezug auf ungewöhnliche E-Mails mit Mailanhängen.
- Erstellen Sie sich einen Notfallordner, ganz klassisch auf Papier. Hier gehören alle wichtigen Unterlagen hinein, zum Beispiel Pläne des Netzwerkes, Notfall-Telefonnummern, gesonderte administrative Kennwörter, aber auch Lizenzcodes von wichtiger Software.
- Stellen Sie sicher, dass Sie alle Installationsmedien für ihre Software besitzen, also beispielsweise für das Betriebssystem, für ein Zugangskontrollsystem, oder auch für betriebswirtschaftliche / kaufmännische Anwendungen.

POLIZEI
Nordrhein-Westfalen
Düsseldorf

- Prüfen Sie die Zugriffsrechte in Ihrem Unternehmen. Auch Angehörige der Geschäftsführung benötigen keinen Zugriff auf alle Daten.
- Erstellen Sie einen Plan für eine Datensicherung, möglichst mit Tages-, Wochen- und Monatssicherungen auf unterschiedlichen Sicherungsmedien.
- Sichern Sie ihre Daten auf unterschiedliche Datenträger, die nie gleichzeitig alle mit dem Computer verbunden sind. Bewahren Sie ihre Sicherungsmedien möglichst in Datensicherungsschränken in einem anderen Brandabschnitt auf.
- Testen Sie regelmäßig, ob eine Rücksicherung bzw. ein Restore funktioniert. Ziehen Sie dabei in Betracht, dass Sie ihre Daten eventuell auf einem völlig anderen/neuen Computer wiederherstellen müssen. Sind ihre Sicherungsmedien auch dort lesbar?
- Erstellen Sie einen Wiederanlaufplan für die IT-Systeme. Gibt es Systeme, die voneinander abhängig sind? Gibt es Systeme, die zuerst eingeschaltet werden müssen?
- Wenn Sie mit einem externen IT-Dienstleister zusammen arbeiten, so prüfen Sie, was durch einen Vertrag für ein Disaster-Recovery abgedeckt ist. Wird nur der Server oder das Rechenzentrum in seinen Grundfunktionalitäten wiederhergestellt, oder auch der Datenbestand?
  Wie lange dauert es, um alle ihre Daten auf einen neuen Server zurückzusichern?

Ransomware/Kryptotrojaner

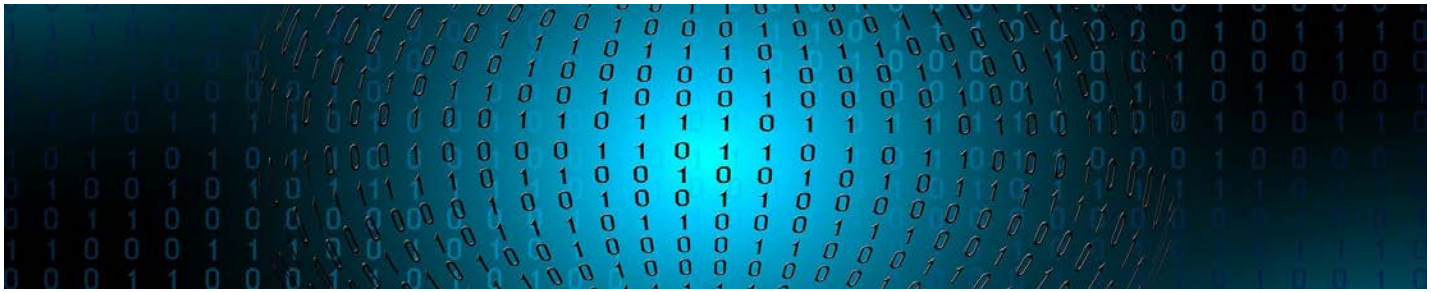
POLIZEI
Nordrhein-Westfalen
Düsseldorf

- Errechnen Sie mögliche Ausfallzeiten. Eine Verfügbarkeitsgarantie von 99,999 % hat immer noch 0,001% Restrisiko. Bei 365 Tagen * 24 Stunden sind das rund 8,76 h Ausfall.

  Je nach Branche können solch ein Produktionsstillstand oder eine unterbrochene Warenabfertigung für „just-in-time“ Lieferungen schon so teuer sein, dass sich ein Back-up-Rechenzentrum lohnt. Beachten Sie, dass auch Stand-by-Systeme, die ständig online sind, Ziel eines Angriffes werden können, insbesondere, wenn administrative Kennwörter in die Hand der Kriminellen gelangen.

- Benennen Sie eine „Taskforce“. Stellen Sie Kompetenzen sicher: Wer beauftragt einen externen IT-Dienstleister? Wer spricht mit der Presse, wer mit der Polizei?
- Führen Sie Übungen durch: Was passiert, wenn alle Server abgeschaltet sind? Kann im Notfall jede mitarbeitende Person im Unternehmen einen Nothalt/Emergency Shutdown der Server durchführen? Was passiert bei einem IT-Ausfall „an ultimo“, z.B. bei einem Monatsabschluss?

Die Homepage des Sachgebietes „Prävention Cybercrime“ des Polizeipräsidiums Düsseldorf finden Sie unter:
https://duesseldorf.polizei.nrw/artikel/cybercrime-2“ https://duesseldorf.polizei.nrw/artikel/cybercrime-2



Impressum

Herausgeber
Polizeipräsidium Düsseldorf
Kommissariat Kriminalprävention/Opferschutz

Luegallee 65
40545 Düsseldorf
Tel.: 0211 - 870 5249
E-Mail: KKKP-O.Duesseldorf@polizei.nrw.de