POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Erpressungsversuche via E-Mail
Präventionshinweise für Betroffene

Erläuterung

Im Phänomenbereich der „Digitalen Erpressung“ gibt es neben den bereits bekannten Varianten der „Ransomware“[1] seit einiger Zeit neue Tatbegehungsweisen, die den Grundsätzen der „Ransomware“ entsprechen.

Die Täter erreichen damit den höchstpersönlichen Lebensbereich ihrer Opfer, indem sie drohen, sexuell belastendes Material zu veröffentlichen.

Die Polizei unterscheidet zurzeit zwei Phänomene.

Sextortion[2] nach Kontaktaufnahme

In diesen Fällen kontaktieren die Täter zunächst ihre Opfer über soziale Medien oder diverse Foren. Sie animieren es, sexuelle Handlungen bei einem Videochat durchzuführen. In vielen Fällen nehmen die Täter das Verhalten des Opfers auf und drohen während des Chats damit, dieses Video zu veröffentlichen.

Sextortion nach Datenleak[3]

Auf der anderen Seite versenden Täter E-Mails, in denen sie behaupten, schon im Besitz kompromittierender Filmaufnahmen zu sein.

In diesen Fällen schreiben sie die Opfer mit Namen an und geben vor, der Rechner, das Smartphone oder ähnliches seien „gehackt“ worden. Die Täter untermauern dies dem Opfer gegenüber, in dem sie ihm sein eigenes Passwort oder Teile seiner Handynummer nennen. Vermeiden kann der Geschädigte das angeblich nur, wenn er einen Geldbetrag in Kryptowährung, in der Regel Bitcoins, auf ein bestimmtes Wallet[4] zahlt.

Oft besitzen die Täter dabei gar kein kompromittierendes Material. Sie haben lediglich im sog. „Dark-Net“ persönliche Daten und Passwörter aufgekauft, die aus Hackingattacken gegen große Provider oder Online-Anbieter stammen.

---

[1] Bei Ransomware handelt es sich um eine Schadsoftware, die – wenn sie auf einem Rechner zur Ausführung kommt – den Zugriff auf das System sperrt oder die Daten so verschlüsselt, dass sie unbrauchbar werden. Für die Freigabe des Systems oder die Entschlüsselung der Daten wird ein Lösegeld verlangt.

[2] Sextortion ist ein Kofferwort, das sich aus dem englischen Wort für Erpressung (Extortion) und Sex ableitet. Es definiert den Modus Operandi, Druck auf ein Opfer mittels Aspekten der Sexualität aufzubauen.

[3] durch einen Anwenderfehler oder Softwarefehler verursachte oder vorsätzlich herbeigeführte Offenlegung vertraulicher Daten.

[4] ist eine virtuelle Geldbörse, die es Nutzern erlaubt, Guthaben auf digitalen Plattformen zu speichern und für Zahlungen im Internet zu verwenden.

Die Polizei gibt folgende Hinweise:

Machen Sie sich stets bewusst, dass Sie während eines Videochats gefilmt werden könnten. Diese Filminhalte könnten ggf. dazu verwendet werden, Sie zu erpressen.

Deaktivieren Sie Ihre Webcam immer, wenn Sie nicht gerade via Videochat mit jemandem sprechen. Wenn Sie ganz sicher gehen wollen, verdecken Sie Ihre Webcam.

Halten Sie das Betriebssystem, den Browser und den Virenschutz Ihrer elektronischen Geräte immer auf dem aktuellsten Stand, um sich vor Malware zu schützen.

Überprüfen Sie Ihre eigene E-Mail-Anschrift mit Hilfe eines sog. „Identity Leak Checker“[1] , ob die jeweils persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden und hierdurch dem Missbrauch preisgegeben sind. Ändern Sie dann Ihre persönlichen Zugangsdaten!

Wenn Sie Opfer geworden sind:

In beiden Fällen sollten Sie nicht in Panik geraten und ohne Schamgefühl Strafanzeige bei der Polizei erstatten. Zahlen Sie auf keinen Fall!

Falls die Erpresser Bild- oder Videomaterial veröffentlicht haben, wenden Sie sich so schnell wie möglich an den betreffenden Dienstanbieter. Verlangen Sie von ihm, die Inhalte umgehend zu löschen.

Überprüfen Sie mit Suchmaschinen Ihren Namen auf neue Videos oder Fotos, die jemand mit Ihrem Namen im Internet hochgeladen hat. Informieren Sie Ihre Bank, um eventuelle Überweisungen (Abbuchungen?) anzuhalten oder rückgängig zu machen.

Ändern Sie sofort alle Passwörter für ihre Zugänge zu Foren, Mail Accounts usw.

Wenn der Vorfall Sie zu sehr belastet, sprechen Sie mit einer Vertrauensperson über den Vorfall oder suchen Sie sich psychologische Hilfe.

Erstatten Sie immer eine Strafanzeige. Nur so bekommt die Polizei Kenntnis von der Straftat und kann die Täter verfolgen. Außerdem erhält sie dadurch Informationen zum Ausmaß der Taten und kann Zusammenhänge herstellen.

Weiterführende Hinweise und Links

Opfer von Straftaten sind nicht auf sich alleine gestellt. Es gibt zahlreiche Beratungsstellen, z. B. die Außenstellen der Verbraucherschutzzentrale NRW.

www.weisser-ring.de

www.vz-nrw.de

https://vimeo.com/219109969/31cc1c2414

Weitere Informationen erhalten Sie unter

www.polizei-beratung.de

www.polizeifürdich.de

Bei weiteren Fragen wenden Sie sich an die für Kriminalprävention und Opferschutz zuständigen Organisationseinheiten in Ihrer Nähe. Den Kontakt finden Sie über https://polizei.nrw/

[1] Internetseiten, auf denen Sie durch Eingabe von E-Mail-Adressen überprüfen können, ob Ihre Adresse bereits im Rahmen zurückliegender Hackerangriffe betroffen war.

https://polizei.nrw/

Herausgeber

Landeskriminalamt Nordrhein-Westfalen

Abteilung 3, Dezernat 32,

Sachgebiet 32.1 - Prävention von Jugend-, Gewalt- und Drogenkriminalität,

Kinder-/Jugend- und Opferschutz und Cybercrime

Völklinger Str. 49

40221 Düsseldorf

Stand

April 2020