Ihre POLIZEI
Votre POLICE
La vostra POLIZIA

Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

SKPPSC

Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

Was ist Sextortion?

Sextortion bezeichnet eine Erpressungsmethode, bei der eine Person mit Bild- oder Videomaterial erpresst wird, das sie nackt oder bei sexuellen Handlungen (Masturbieren) zeigt. Die überwiegende Mehrheit der Opfer von Sextortion ist männlich. Es handelt sich dabei sowohl um Jugendliche als auch Erwachsene. Häufig finden die Chats in gebrochenem Deutsch, Französisch oder Englisch statt. Die Täterinnen und Täter befinden sich im Ausland und auch die Geldzahlungen gehen auf ausländische Konten. Es gibt immer wieder Fälle, in denen die Opfer die geforderte Geldzahlung geleistet haben, aber das kompromittierende Material dennoch veröffentlicht wird oder erneute Forderungen gestellt werden.

Drei verschiedene Varianten

Die klassische Variante: Die Zielpersonen erhalten über soziale Netzwerke eine Freundschaftsanfrage oder eine Einladung einer verführerischen Unbekannten. Nach der Annahme dieser Einladung oder Anfrage nimmt die neue virtuelle Freundin via Chat Kontakt mit der Zielperson auf und verwickelt sie in ein Gespräch. Sie schlägt vor, in einen Videochat wechseln. Dort bringt sie die Zielperson dazu, sich auszuziehen, zu masturbieren, nackt herumzutanzen oder anzüglich zu posieren. Die unbekannte Verführerin gaukelt der Zielperson vor, dass sie sie sehr attraktiv findet, sexuell erregt ist und selbst einen sehr lockeren Umgang mit Nacktheit und Masturbation hat. Um glaubhaft zu wirken, macht sie den ersten Schritt, indem sie ihre Brüste zeigt oder beginnt, sich vor der Zielperson zu befriedigen. Ohne dass die Zielperson es bemerkt, werden all ihre Handlungen während des Videochats aufgezeichnet. Kurze Zeit später wird sie von Erpressern kontaktiert und zu einer Geldzahlung aufgefordert. Sollte sie dies nicht tun, würden die Aufnahmen verbreitet.

Im Videoclip des ersten Teils der nationalen Präventionskampagne vom 26. März 2020 wird die Geschichte von Leo und seinen ernüchternden Erfahrungen mit der fiktiven Anna erzählt. Er ist ein Opfer dieser klassischen Variante von Sextortion.

Die Malware-Variante: Bei dieser Form von Sextortion werden die Computer, Tablets und Smartphones von Personen, die auf präparierten Webseiten mit pornografischen Inhalten surfen, mit einer Malware infiziert. Die Malware aktiviert die Webcam der Geräte und filmt die ahnungslosen Opfer, während sie Pornos schauen. Die häufig kompromittierenden Filmaufnahmen werden an die Täterschaft übermittelt und die Opfer werden anschliessend unter der Androhung, dieses Filmmaterial zu veröffentlichen oder an die ebenfalls gestohlenen Freundeslisten zu versenden, erpresst.

Die Spam-Variante: Es kommt auch vor, dass diese Erpressungsversuche «leere Drohungen» sind, die als Spam an zahlreiche Personen versendet werden. Die kriminellen Absender hoffen, dass sich unter

den Empfängern tatsächlich Personen befinden, die sich in letzter Zeit Pornos geschaut haben, und dass diese sich durch die Androhung einschüchtern lassen und deshalb zahlen. In diesen Fällen ist der Computer der Betroffenen weder infiziert, noch ist die Täterschaft tatsächlich in Besitz von kompromittierendem Material.

Einige Zahlen

Es gibt keine offizielle schweizweite Statistik für Sextortion im Allgemeinen. Allerdings wurde alleine für die Spam-Variante zwischen Juli 2018 und Dezember 2018 eine Vervielfachung der Fälle beobachtet. Basierend auf der Analyse der Bitcoin-Adressen in den E-Mails, die der Melde- und Analysestelle Informationssicherung MELANI gemeldet wurden, sind in der zweiten Jahreshälfte 2018 fast 100 Bitcoins einbezahlt worden, was im damaligen Zeitpunkt einem Betrag von rund 360'000 Franken entsprochen hat. Dieser Gewinn ist umso grösser, als der Versand von Massen-E-Mails praktisch nichts kostet.

Zudem wurden Anfang 2019 innerhalb von nicht einmal fünf Tagen Bitcoins im Wert von über 400'000 Franken auf ein einziges Konto einbezahlt, das im Zusammenhang mit einer grossen Sextortion-Welle in deutscher Sprache verwendet wurde. Diese Welle löste Hunderte von Meldungen an MELANI aus. Aufgrund der Sprache ist davon auszugehen, dass sie die deutschsprachigen Länder im Visier hatte. Die Verknüpfungen einzelner Bitcoin-Adressen lassen im Übrigen darauf schliessen, dass es sich bei mindestens fünf Spam-Wellen, die am 7. Januar 2019 starteten, um eine einzelne Kampagne handelt, auch wenn sich die E-Mails in Sprache und Typ unterscheiden.

Was können Sie tun?

Bei der klassischen Variante:

Damit Sie kein Opfer werden:

- Nehmen Sie keine Freundschaftsanfragen und Einladungen in sozialen Netzwerken an, wenn Sie die Person nicht zweifelsfrei identifizieren können oder im realen Leben bereits getroffen haben.
- Machen Sie sich stets bewusst, dass Sie während eines Videochats gefilmt werden könnten, und verzichten Sie deshalb auf Handlungen, für welche Sie sich im Nachhinein schämen könnten.
- Deaktivieren und überkleben Sie Ihre Webcam immer, wenn Sie nicht gerade via Videochat mit jemandem sprechen.
- Halten Sie das Betriebssystem, den Browser und den Virenschutz Ihrer elektronischen Geräte immer auf dem aktuellsten Stand, um sich vor Malware zu schützen
- Informieren Sie Ihr Umfeld über diese Erpressungsmethode.

Wenn Sie Opfer geworden sind

- Gehen Sie nicht auf die Forderung der Erpresser ein: Zahlen Sie nicht!
- Brechen Sie den Kontakt zur Frau und zu den Erpressern sofort ab. Löschen Sie sie aus Ihrer Freundesliste und reagieren Sie nicht auf ihre Nachrichten.
- Falls die Erpresser Bild- und Videomaterial veröffentlicht haben, wenden Sie sich so schnell als möglich bei der betreffenden Plattform und verlangen Sie umgehend die Löschung der sexuellen Inhalte.
- Richten Sie einen Google Alert mit Ihrem Namen ein. Auf diese Weise werden Sie über neue Videos und Fotos, die mit Ihrem Namen im Internet hochgeladen werden, informiert.
- Sichern Sie alle Beweise und erstatten Sie Anzeige bei Ihrer Polizei.
- Sprechen Sie mit einer Vertrauensperson über den Vorfall oder suchen Sie sich psychologische Hilfe

Bei der Malware-Variante:

- Zahlen Sie nicht, auch wenn die Erpresser sich mehrmals und eindringlich melden!
- Überprüfen Sie Ihren Computer auf Malware oder lassen Sie ihn von einer Fachperson überprüfen und gegebenenfalls neu aufsetzen.
- Ändern Sie alle Ihre Passwörter und achten Sie darauf, gute und verschiedene Passwörter zu wählen.

Zitate von Opfern[1]

«Es ist ihr sehr rasch gelungen, mein Vertrauen zu gewinnen, und ich habe mich wirklich total reinlegen lassen.»

«Was sie wollte, war nur Geld. Ich bin grundsätzlich ein sehr gestresster Mensch, deshalb hat mich das enorm belastet. Aber ich habe alles für mich behalten. Ich habe mich abgekapselt und dann, na ja, dann habe ich halt nachgegeben.»

«Sie sagte mir, sie habe es [das Geld] erhalten, aber sie wolle noch mehr.»

«Ich hatte Selbstmordgedanken. Ich war völlig verzweifelt.»

«Ja sicher, ich habe eine schlechte Erfahrung gemacht. Aber wenigstens soll diese als Warnung und zur Prävention dienen. Das ist besser, als nichts zu sagen und niemandem zu helfen.»

[1] Zitate von Opfern auf YouTube, veröffentlicht von der Kantonspolizei Neuenburg am 20. Mai 2015