Humanitas Helvetica e.V.
Newsletter

Sextortion - Sexuelle Erpressung im Internet

Der Begriff „Sextortion“ (Wortkombination aus „Sex“ und „Extortion“ = Erpressung), bezeichnet eine Betrugsmasche im Internet. Erpresser behaupten in einer Mail, Zugang zu Computer und Webcam zu haben und drohen damit, Bilder und Videos mit sexuellem Inhalt zu veröffentlichen, sollte kein Lösegeld bezahlt werden. Diese Betrugsmasche wird Fake-Sextortion genannt und dabei wird typischerweise eine Bezahlung in Bitcoins gefordert. Mit dieser Betrugsmethode haben Kriminelle in den letzten sechs Monaten trotz der kleinen geforderten Summen Bitcoins im Wert von zirka 360‘000 CHF erbeutet. Solange die betroffenen E-Mail-Empfänger Lösegeld bezahlen, wird dieses Vorgehen befeuert und weiterhin eingesetzt.

Die Betrugsmasche «Fake-Sextortion» besteht darin dem Opfer vorzugaukeln, dass Kriminelle Zugang zu dessen Webcam hätten und es beim Konsum von Pornographie gefilmt worden sei. Wird nicht innerhalb einer Frist ein bestimmter Betrag an Bitcoins bezahlt, drohen die Erpresser damit, die Videos allen Kontakten des Empfängers zuzustellen. Als Beweis für die Kompromittierung des Computers wird meist ein Passwort aus einem Datenabfluss angegeben.

In den meisten Fällen ist dieses Passwort jedoch veraltet und nicht mehr in Gebrauch. Mittlerweile werden diverse andere Varianten beobachtet: So werden auch Mobilfunknummern verwendet, um das Opfer zu überzeugen, dass das Mobiltelefon kompromittiert worden sei. In einer anderen Variante wird als Beweis, dass das eMail-Konto kompromittiert worden sei, die Nachricht scheinbar mit der eigenen Mailadresse versendet.

In Tat und Wahrheit ist der Absender jedoch gefälscht, was sehr einfach und ohne grosse Kenntnisse gemacht werden kann. Eine Unterart dieses Phänomens sind gefälschte Erpressungen mit Androhung eines Säure- oder Bombenanschlags. Bei beiden Varianten sollten Bitcoins bezahlt werden, um den Anschlag zu verhindern. Erpresser-eMails werden in mehreren Sprachen versendet, darunter auch Deutsch, Französisch, Italienisch und Englisch. Obwohl ihr Modus Operandi sich im Grossen und Ganzen nicht verändert hat, arbeiten die Kriminellen kontinuierlich daran, ihre Erpressungsversuche anzupassen, um den Druck auf die Opfer zu erhöhen und sie zum Bezahlen zu nötigen.

360‘000 CHF auf Bitcoin-Konten, die MELANI gemeldet wurden

Fake-Sextortion (Fake, da es sich um einen Bluff handelt und keine kompromittierenden Bilder existieren) wird vermehrt seit Juli 2018 beobachtet. Basierend auf der Analyse der Bitcoin-Adressen in den eMails, die MELANI gemeldet wurden, sind in der zweiten Jahreshälfte 2018 fast 100 Bitcoins einbezahlt worden, was derzeit einem Gegenwert von ungefähr CHF 360‘000 entspricht. Ausgehend davon, dass der Versand von Massen-eMails praktisch kostenlos ist, ist der Gewinn entsprechend hoch. Ob die Bitcoin-Adressen ausschliesslich für Fake-Sextortion verwendet werden, ist nicht bekannt.

Weltweit 22 Millionen erbeutet

Die Sicherheitsorganisation SANS publizierte kürzlich einen Tweet, dass ein Bitcoin-Konto mit USD 22 Millionen in Zusammenhang mit Fake-Sextortion entdeckt wurde.

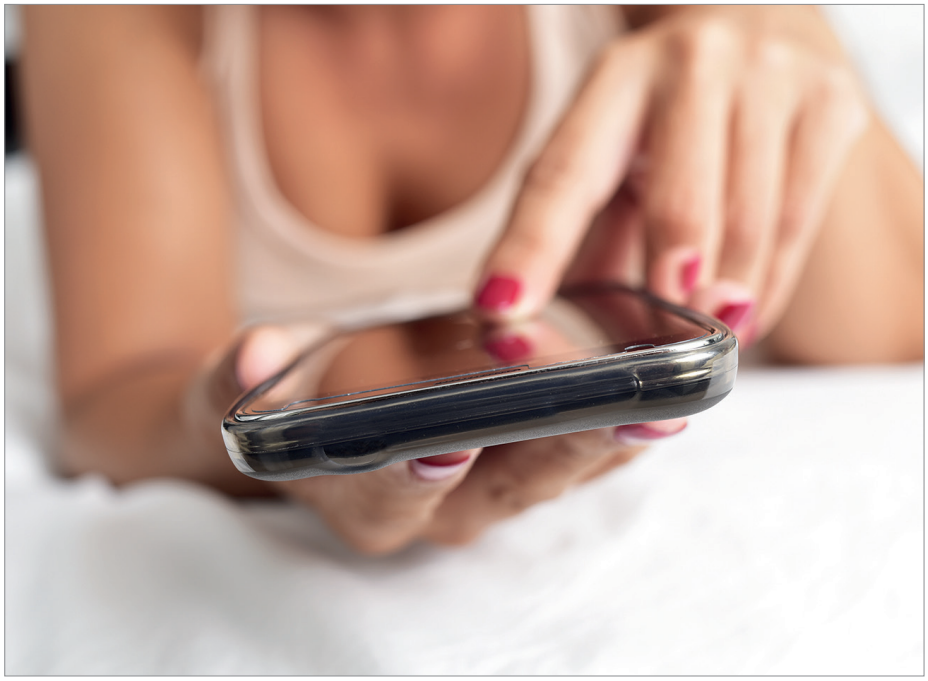
Sextortion - ein Millionen-Geschäft. (Bild © Florian; #156551231; - stock.adobe.com)

Kein Lösegeld bezahlen!

Die Ursache, wieso so viele Leute das geforderte Lösegeld bezahlen, dürfte darin liegen, dass gerade Personen, die tatsächlich Pornographie konsumieren, sich schämen und sich durch solche Erpressungsversuche verängstigen lassen, deshalb nicht darüber sprechen und die Erpressung auch nicht melden. Umso mehr, da es sich meist um relativ kleine Lösegeldforderungen handelt.

Solange die betroffenen Empfänger allerdings nicht aufhören, Lösegeld zu bezahlen, wird diese Masche befeuert und es wird erwartet, dass diese Wellen weitergehen, dass Nachahmungstäter auf den Zug aufspringen und die Anzahl noch weiter zunehmen wird.

Zahlen Sie deshalb unter keinen Umständen ein Lösegeld. Sie können zur Prävention beitragen, indem Sie diese Vorgehensweise von Kriminellen in Ihrem beruflichen und persönlichen Umfeld thematisieren. Sensibilisieren Sie Mitarbeiter, Bekannte und Verwandte, damit sie nicht auf solche Machenschaften hereinfallen.



In gewissen Fällen sollte die Kamera deaktiviert sein. (Bild © nito; #90053098; - stock.adobe.com)

Verhaltensregeln

In der Melde- und Analysestelle Informationssicherung MELANI des Bundes arbeiten Partner zusammen, welche im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen kritischen Infrastrukturen tätig sind.

Neben technischen Massnahmen (z. B. Personal Firewall, Software-Updates, Antiviren-Software, usw.) zur Erhöhung der Sicherheit eines Rechners, ist vor allem das Verhalten jedes einzelnen Benutzers von entscheidender Bedeutung.

Hinsichtlich eMail-Verkehr empfiehlt MELANI unter anderem:

eMail ist eines der beliebtesten Kommunikationsmittel. Allerdings gelangen die meisten elektronischen Schädlinge über eMail-Anhänge auf den Rechner. Ein sorgsamer Umgang mit eMails trägt erheblich zur Sicherheit Ihrer Daten und Ihres Rechners bei. Folgende Massnahmen schützen gegen Viren, Würmer, Trojanische Pferde, Spam und Hoaxes:

Vorsicht bei eMails mit unbekanntem Absender: Misstrauen Sie eMails, deren Absenderadresse Sie nicht kennen. Öffnen Sie in diesem Fall keine angefügten Dokumente oder Programme und klicken Sie keine darin angegebenen Links an.

Auf Vertrauenswürdigkeit der Quellen achten: Öffnen Sie nur Dateien oder Programme aus vertrauenswürdigen Quellen und nur nach vorgängiger Prüfung mit einer aktuellen Antiviren-Software.

Vorsicht bei Dateinamen mit zwei Endungen: Öffnen Sie keine eMail-Anhänge, die zwei Endungen aufweisen (z. B. picture.bmp.vbs). Lassen Sie sich nicht durch das Icon einer solchen Datei täuschen. Deaktivieren Sie im Windows Explorer die Option «Erweiterungen bei bekannten Dateitypen ausblenden», respektive «Hide file extensions for known file types».

Software-Update des eMail-Programms: Auch eMail-Programme können Sicherheitslücken aufweisen. Vergewissern Sie sich regelmässig, ob ein Software-Update Ihres eMail-Programms vorhanden ist und spielen Sie dieses ein.

Vorsichtiger Umgang mit der eMail-Adresse: Geben Sie Ihre eMail-Adresse nur an so wenige Personen wie notwendig weiter und verwenden Sie diese ausschliesslich für wichtige Korrespondenz.

Anlegen einer zweiten eMail-Adresse: Für das Ausfüllen von Webformularen, das Abonnieren von Newslettern, Einträge in Gästebüchern, usw. empfiehlt es sich, eine zweite eMail-Adresse zu verwenden. Diese kann bei verschiedenen Anbietern kostenlos beantragt werden. Ist diese Adresse von Spam betroffen, kann sie gelöscht und ersetzt werden.

Spam nicht beantworten: Wird auf Spam geantwortet, so weiss der Sender, dass die eMail-Adresse gültig ist und wird weiter Spam verschicken. Mit Vorsicht ist auch Spam mit «Abbestelloption» zu geniessen. Darin wird versprochen, dass man durch Senden einer eMail mit bestimmtem Inhalt von der Verteilerliste gestrichen wird. In diesem Zusammenhang sind auch automatische Antwortmails bei Ferienabwesenheit zu beachten. Sie sollten lediglich bei bekannten Adressen aktiviert werden.

Mindestlänge von 12 Zeichen: Die Mindestlänge des Passwortes sollte bei 12 Zeichen liegen und sowohl aus Buchstaben, Zahlen wie auch Sonderzeichen bestehen.

Einfach zu merken: Das Passwort ist so zu wählen, dass man es sich einfach merken kann. Schreiben sie keine Passwörter auf. Gute Passwörter bestehen aus ganzen Sätzen, die ebenfalls Sonderzeichen enthalten. Beispiel: «Dieses P@ssw0rt vergesse 1ch nie!!»

Passwort nicht mehrfach verwenden: Verwenden Sie verschiedene Passwörter für verschiedene Zwecke (z. B. für unterschiedliche Benutzerkonten). Bei der Nutzung von Online-Diensten wird dringend empfohlen, jeweils andere Passwörter zu verwenden.

Passwort regelmässig ändern: Ein Passwort sollte in regelmässigen Abständen (ca. alle 3 Monate) gewechselt werden, jedoch spätestens dann, wenn Sie vermuten, dass es Dritten bekannt sein könnte.

Starke (zwei Faktor) Authentifizierung: Schützen Sie den Zugang zu Ihren Internetdiensten falls verfügbar mit einer Zwei-Faktor Authentifizierung (Einmal Passwort, SMS-Token, Authenticator usw.)

Weitere Ratschläge siehe MELANI-Website: www.melani.admin.ch

www.stop-sextortion.ch

Die Behörden haben eine Webseite - www.stop-sextortion.ch - lanciert, dort finden Sie Informationen und können Fake-Sextortion eMails melden. ●

Kinderpornografie - Täter und Opfer

Laut Presse hat die amerikanische Bundespolizei (FBI) der Schweiz letztes Jahr rund 9'000 Fälle von mutmasslicher Kinderpornografie gemeldet - so viele wie noch nie. Das Fedpol hat nach Prüfung der Hinweise weniger als zehn Prozent der Fälle an kantonale Behörden weitergeleitet. Kürzlich haben wir in einer Broschüre „Kinderschutz" das Thema beschrieben. Auszüge daraus sind:

Die Broschüre «Kinderschutz - Dokumentation über Gewalt und Gefahren» finden sie in der Online-Version auf unserer Homepage www.humanitas-helvetica.ch. Print-Versionen können Sie kostenlos via eMail info@humanitas-helvetica.ch unter Angabe von Anzahl und Lieferadresse bestellen.

Es bedarf wohl keiner Erklärung was Pornografie ist. Schon diffiziler ist der Begriff Kinderpornografie, denn der wird in verschiedenen Ländern unterschiedlich interpretiert. Ist das Fotografieren eines nackten Säuglings bereits Kinderpornografie oder nicht? Fallen „künstlerische" Fotos oder Gemälde nackter Kinder bereits in die Kategorie? Ist das Nacktfoto einer jungen Ehefrau unter 14 Jahren (was in einigen aussereuropäischen Ländern erlaubt ist) Kinderpornografie?

Die Täter

Die Konsumenten von kinderpornografischen Darstellungen sind fast ausschliesslich Männer. Eine Teil von ihnen (lt. einer deutschen Studie ca. 10%) haben pädophile Erfahrungen. Die Mehrheit ergötzt sich nur an den Darstellungen. Auch homoerotische Neigungen scheinen in der Konsumentengruppe vorhanden zu sein, denn die Mehrheit der kindlichen Darsteller sind Buben.

Bei den Produzenten dieser Produkte muss man vier Gruppen unterscheiden.

- Da sind an erster Stelle Pädophile die ihre eigenen Handlungen filmen oder fotografieren. Üblicherweise wird diese Art von Filmen als Tauschmaterial an entsprechenden Börsen gehandelt.
- Die Gruppe der ausschliesslich an finanziellem Gewinn interessierten Personen, die oft auch sehr professionell agiert, ist rückläufig und in Europa kaum mehr vertreten.
- Die dritte Gruppe umfasst Personen, die an Kindern sexuelle Gewalt ausüben und diese Tat dazu noch filmen. Die Täter sind eigentlich nicht Pädophil, sondern einfach an Gewalt interessiert.
- Die vierte Gruppe ist die wohl abstossendste überhaupt. Es sind jene Eltern die ihre Kinder für derartige Darstellungen gegen finanzielle Abgeltung für sexuelle Handlungen vermieten. Derartige Täter findet man vor allem in den ärmsten Ländern dieser Erde.

Die Täter und ihre Machwerke kommen aus allen Ländern und Kontinenten. Zentren findet man aber in Osteuropa und Südostasien. Die Armut in diesen Ländern und damit die Verlockung eine finanzielle Abgeltung zu bekommen, sind sicher dafür ausschlaggebend. Wie bei vielen Spielarten der gewaltsamen Sexualität, kursieren auch im Bereich Kinderpornografie viele, kaum überprüfbare Gerüchte. So sind keine Fälle bekannt, dass Kinder entführt wurden um mit ihnen Kinderpornos zu drehen. Es ist lediglich auch ein sogenannter Snapchat Film (Tötung eines vergewaltigten Opfers) bekannt.

Die Opfer

Wie bereits angeführt sind es unter 14jährige beiderlei Geschlechtes. Vereinsamte und verwahrloste Kinder sind häufiger Opfer als jenen die in geordneten Verhältnissen aufwachsen. In der überwiegenden Anzahl der Fälle sind es persönliche Beziehungen oder subtiler Druck, der Kinder dazu bringt sich „freiwillig" als Darsteller in einem Pornofilm zu zeigen. Finanzielle Gründe sind eher selten. In der Regel treten bei kinderpornografischen Filmen ein Erwachsener als Täter und ein Kind als Opfer auf, es sind aber Filme vorhanden, wo Kinder untereinander sexuelle Handlungen begehen.

Wie die derzeitige Situation ist und welche Trends sichtbar sind erklärt Chefinspektor **Harald Gremel** vom Bundeskriminalamt Wien in einem Interview in unserer Broschüre «Kinderschutz» ●

Impressum

Humanitas Helvetica e.V. - Newsletter

Herausgeberin
Humanitas Helvetica e.V.
Mimosenstrasse 5, 8057 Zürich
http://www.humanitas-helvetica.ch

Verantwortlicher Redaktor
Hans-Ulrich Helfer
helfer@humanitas-helvetica.ch

Layout, Website
Swisswebmaster GmbH
info@swisswebmaster.ch

Erscheinungsweise
Regelmässig als Print- oder Online-Ausgabe.

Bezug, Unterstützung
Website: www.humanitas-helvetica.ch
Unkosten- und Unterstützungsbeiträge bitte auf Postcheckkonto: 85-587554-5:
IBANCH50 0900 0000 8558 7554 5
Vermerk: „Spende"

Druck
Eigendruck

Kindesmissbrauch
Schweigen oder Anzeigen?

Humanitas Helvetica e.V.
www.humanitas-helvetica.ch