Sextortion

Das Phänomen „Sextortion“ leitet sich aus den Begriffen „Sex“ und „Extortion“ (engl. für Erpressung) ab. Dabei versuchen Betrüger, Internetnutzer mit (vermeintlichen) erotischen Fotos oder Videos zu erpressen.

Vorgehensweise

Bei dieser Betrugsmasche geht es den Tätern darum, Geld von den Opfern zu erpressen. Sie drohen damit, anzügliches Foto- und Videomaterial zu veröffentlichen, wenn nicht gezahlt wird. Opfer sind sowohl Männer als auch Frauen. Die Täter bedienen sich zweier unterschiedlicher Vorgehensweisen:

Variante 1

Bei der ersten Variante wird zunächst Kontakt über soziale Netzwerke aufgenommen, etwa über eine Freundschaftsanfrage bei Facebook. Im Anschluss macht der wortgewandte Täter dem Opfer Komplimente zu seinem Aussehen und beginnt zu flirten. Es folgt ein erotischer Chat mit dem Opfer, in dessen Verlauf der Betroffene auch Nacktbilder oder -videos von seinem Gegenüber geschickt bekommt. Das Ziel: Das Opfer dazu zu bringen, sich vor der Webcam auszuziehen oder sexuelle Handlungen an sich vorzunehmen. Der Täter nimmt das Ganze auf und erpresst das Opfer im Anschluss damit. So wird etwa gedroht, das aufgenommene Video an die gesamte Facebook-Freundesliste zu senden.

Variante 2

Bei der zweiten Betrugs-Variante nutzen die Erpresser Daten, die aus Hacking-Angriffen gegen große Provider oder Online-Dienstleister stammen und über das Darknet vertrieben werden. Die Täter kaufen diese Daten und drohen Betroffenen in E-Mails mit der Veröffentlichung von Nacktbildern oder -videos, die das Opfer angeblich bei sexuellen Handlungen zeigen. Sie behaupten, den Computer der Betroffenen gehackt und damit Zugriff auf die Webcam erhalten zu haben. Als angeblichen Beweis präsentieren die Täter dann Passwörter oder persönliche Daten der Betroffenen. Bei dieser Vorgehensweise sind die Täter in der Regel nicht wirklich in Besitz von anzüglichem Material. Sie setzen aber darauf, dass der Betroffene verunsichert wird und die geforderte Summe bezahlt.

Schutzmaßnahmen

- Gehen Sie mit vertraulichen und privaten Daten, Bildern und Videos grundsätzlich zurückhaltend um.
- Überprüfen Sie Ihre Privatsphäre-Einstellungen bei Facebook und anderen sozialen Netzwerken.
- Bedenken Sie: Hinter einem Internetprofil kann eine andere Person stecken. Seien Sie vorsichtig, wenn eine fremde Person Kontakt aufnehmen möchte.
- Kleben Sie Ihre Webcam ab, wenn sie nicht genutzt wird.

Wenn Sie erpresst werden:

- Brechen Sie den Kontakt sofort ab und lassen Sie sich nicht unter Druck setzen.
- Zahlen Sie auf keinen Fall den geforderten Betrag.
- Erstatten Sie umgehend Strafanzeige bei der Polizei.
- Machen Sie Screenshots vom Account des Täters und sichern Sie Chat-Protokolle oder den E-Mail-Verkehr für spätere Ermittlungen.

Siehe auch:
Betrug
Darknet
Malware/Spyware

Zurück

© Verlag Deutsche Polizeiliteratur