WAS TUN BEI ERPRESSUNGSVERSUCHEN PER MAIL? 7 EINFACHE SCHRITTE GEGEN „SEXTORTION“

Ein Leitfaden für Angestellte

1. Lassen Sie sich nicht aus der Ruhe bringen.

Die Urheber sogenannter Sextortion-Attacken wissen um menschliche Schwächen und bedienen sich der Angst ihrer Opfer, um sie zu unbedachten Reaktionen zu verleiten. Wenn Sie eine entsprechende E-Mail erhalten, sollten Sie deshalb zuallererst davon ausgehen, dass keine der darin getroffenen Aussagen der Wahrheit entspricht. Ziehen Sie im Zweifelsfall immer die interne IT-Abteilung oder den technischen Support ihres Sicherheitsanbieters zu Rate.

2. Zahlen Sie auf keinen Fall Lösegeld.

Hinter den meisten Sextortion-Angriffen stecken schlicht Betrüger, die in Wahrheit keinerlei belastendes Material von Ihnen besitzen. Auch Drohungen, die Polizei einzuschalten oder Sie anderweitig Ihrer „Strafe“ zuzuführen, sind natürlich Unsinn. Zahlen Sie deshalb auf keinen Fall geforderte Lösegelder – so fördern Sie lediglich das „Geschäftsmodell“ der Angreifer und helfen ihnen, weitere, ähnliche Attacken durchzuführen.

3. Reagieren Sie nicht auf die E-Mail.

Antworten Sie nicht auf die Nachricht, laden Sie keinerlei Anhänge herunter und klicken Sie nicht auf Links oder ähnliche Inhalte, da sich hier Malware oder andere Bedrohungen verbergen können.

4. Prüfen/ändern Sie Ihre Passwörter.

Kriminelle nutzen Zugangsdaten aus Datenlecks, um Zugang zu Benutzerkonten zu erhalten und von dort aus weitere Erpressungsmails zu versenden oder andere, gefährlichere Attacken durchzuführen. Enthält eine erpresserische E-Mail also Passwörter, die Sie tatsächlich noch nutzen, ändern Sie diese unverzüglich und aktivieren Sie möglichst eine Zwei-Faktor-Authentifizierung, um Ihre Daten in Zukunft noch umfassender zu schützen.

5. Leiten Sie die E-Mail an Ihre IT-Abteilung weiter.

In manchen Unternehmen werden Spam- und vergleichbare E-Mails als Sicherheitsvorfall gewertet und müssen den entsprechenden internen Stellen gemeldet werden. Vor allem in kleineren Unternehmen, deren IT durch externe Dienstleister abgesichert wird, sind die Mitarbeiter aufgefordert, Vorfälle dem Sicherheitsanbieter zu melden und dessen Anweisungen Folge zu leisten. Besitzt Ihr Unternehmen weder internes noch externes Personal für IT-Sicherheit, so sollten Sie zumindest den betroffenen Rechner und das Netzwerk mithilfe einer zuverlässigen Security-Lösung überprüfen und sicherstellen, dass keines der von Ihnen verwendeten Passwörter gestohlen oder kompromittiert wurde.

6. Sichern Sie Ihre Webcam.

Sorgen Sie dafür, dass Ihre Webcam nicht durch Angreifer missbraucht werden kann, indem Sie sie mithilfe von Sicherheitssoftware schützen oder zumindest vorsichtig abkleben oder abdecken. So können Sie sicher sein, dass sie Sie nicht unbemerkt aufnimmt.

7. Verwenden Sie einen Spam-Schutz.

Um in Zukunft Spam und andere unerwünschte E-Mails von Ihrem Postfach fernzuhalten, nutzen Sie eine Sicherheitslösung mit integriertem Spam-Schutz.

eset