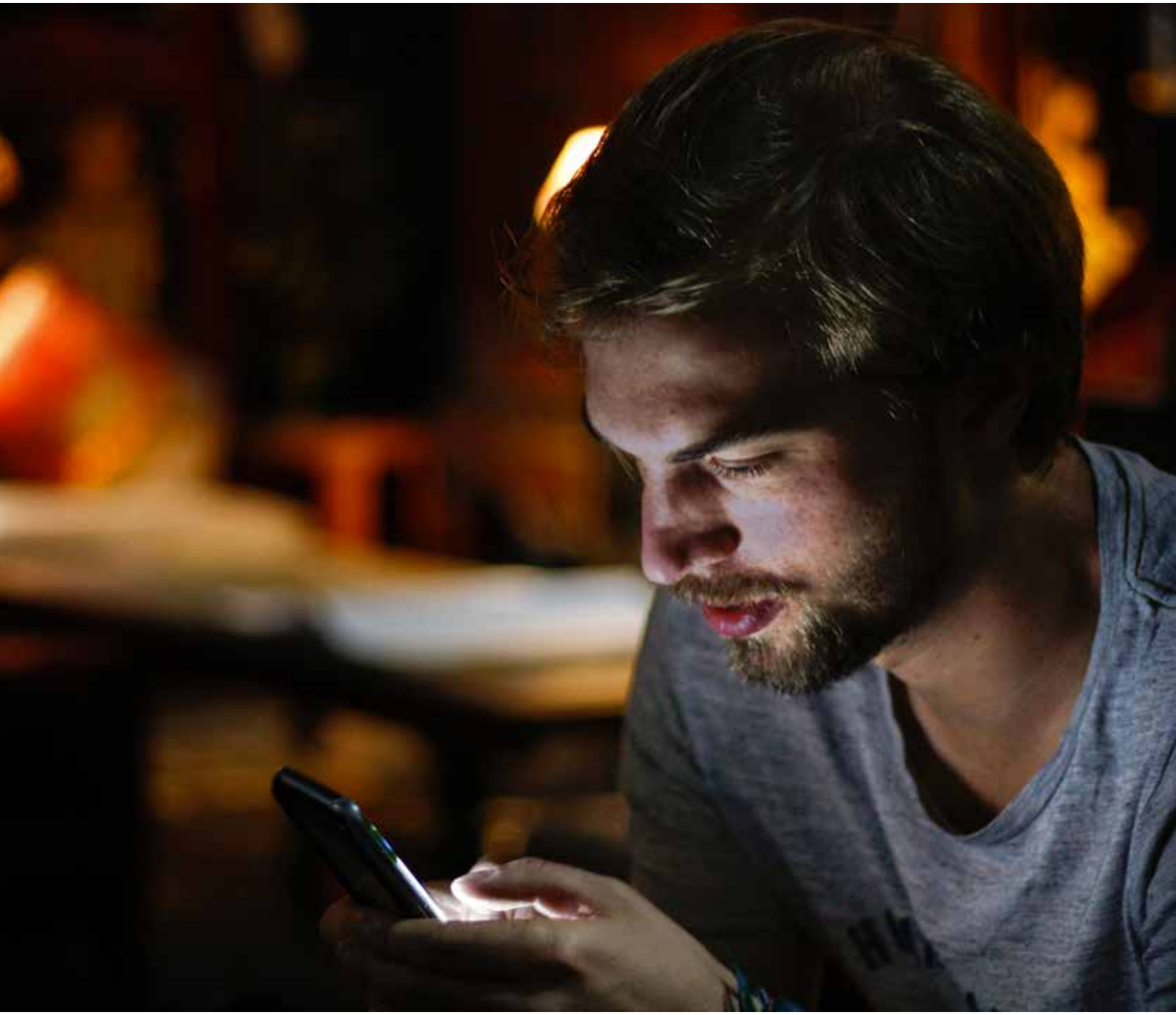
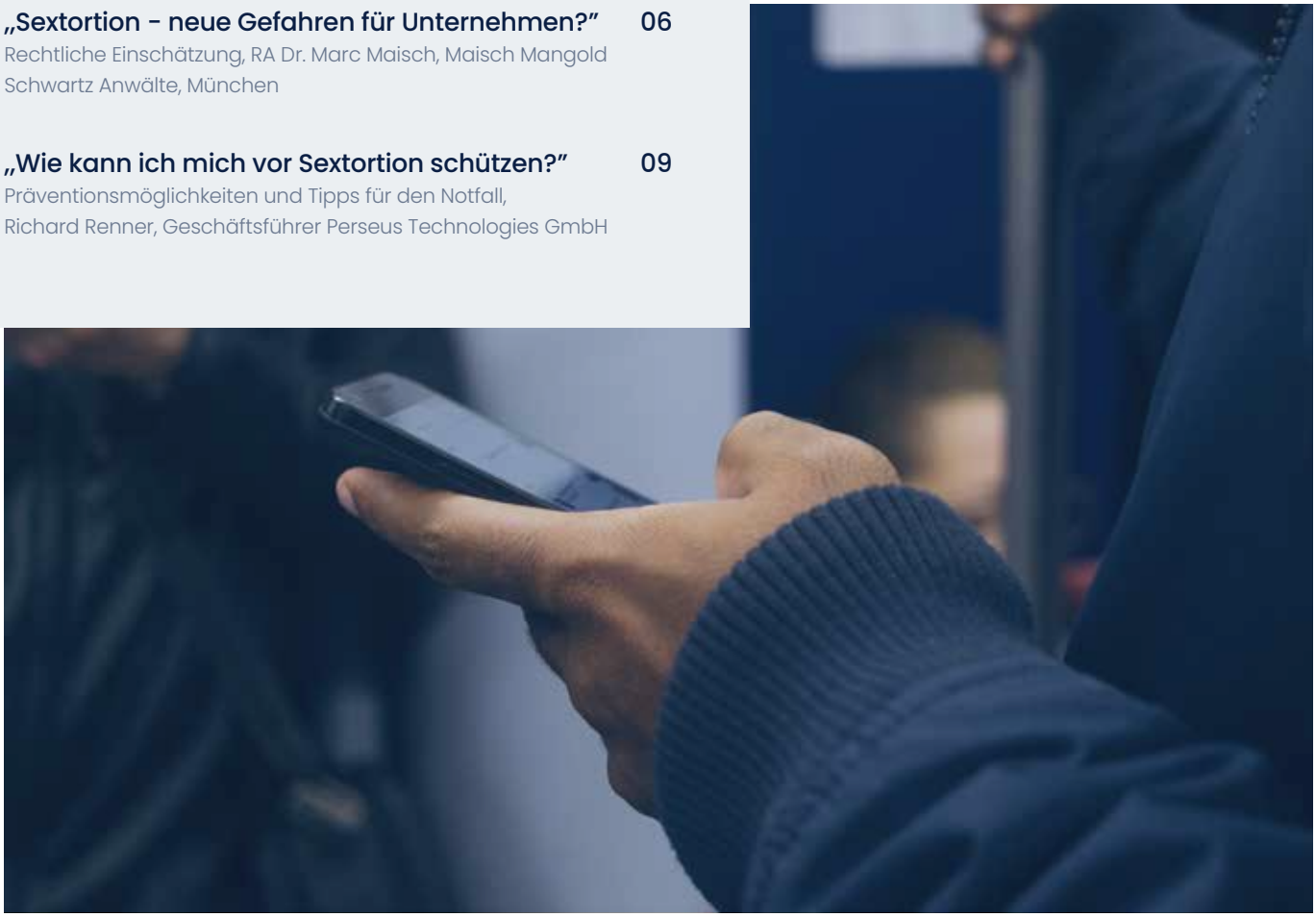


Whitepaper: Sextortion

„Ich weiß, was Sie getan haben…."

perseus.
Cybersicherheit auf den Punkt

Inhalt



Interview mit Esther Papp

Esther Papp | Polizeipräsidium München

Nach dem Abitur 1989 begann sie ihre Ausbildung bei der weiblichen Kriminalpolizei in München. Sie war langjährige Sachbearbeiterin bei den Kommissariaten für Vergewaltigung/Sex, Missbrauch und Häuslicher Gewalt/Stalking/Misshandlung Schutzbefohlener. Seit 2012 ist sie Beraterin und Speaker beim Opferschutz des Polizeipräsidiums München. Esther Papp ist Mitglied von Blackstone432 (www.blackstone432.de).

Was verstehen Sie unter dem Begriff „Sextortion“?
Unter Sextortion versteht man sexuelle Erpressung. Personen werden mit vermeintlichen Aufnahmen erpresst, auf denen sie sexuelle Handlungen vor der Webcam vorgenommen haben sollen. Erst gegen eine Geldzahlung wird die Verbreitung der Aufnahmen durch die Erpresser unterlassen.

Wie viele Fälle von Sextortion gibt es in Deutschland?
Es gibt dazu keine konkreten Zahlen. Erstens ist das Dunkelfeld sicher groß, viele Leute erstatten aus Scham keine Anzeige. Zweitens kann es in der Kriminalstatistik aufgrund der allgemeinen Erfassung als Erpressung nicht gesondert ausgewertet werden. Entsprechend sind auch keine Zahlen zu den wirtschaftlichen Schäden durch Sextortion-Erpressungen bekannt.

Gibt es eine Zielgruppe, die besonders betroffen ist? Suchen die Täter beispielsweise auch nach Personen, die in Managementpositionen oder Geschäftsinhaber sind?
Bei Sextortion handelt es sich zwar um eine “Massenphänomen”, d.h. Die E-Mails an mehrere Personen gleichzeitig. Die Zielgruppe sind dennoch vorrangig Männer, unabhängig von der beruflichen Position.

Haben Sie selbst schon mal eine solche E-Mail bekommen?
Nein, bisher bin ich davon verschont geblieben :)

Was bedeutet es für die IT-Sicherheit, wenn man eine Sextortion-E-Mail bekommt?
Für die IT-Sicherheit spielen diese E-Mails keine Rolle. Es geht dabei nicht um das Erspähen oder Abgreifen von Daten oder den Versand von Trojanern. Aus unternehmerischer Perspektive kann es bei Sextortion-Fällen vor allem dann zu einem finanziellen Schaden kommen, wenn durch Unwissenheit, Angst und Scham ein Lösegeld gezahlt wird.

Wie unterscheidet sich ein „Racheporno“ von „Sextortion“?
Beim „Racheporno“ geht es eher darum, dass Personen von ihren ehemaligen Sexpartner emotional geschädigt oder unter Druck gesetzt werden. Meist sind die “Verflossenen” gekränkt und wollen sich rächen. Sextortion zielt auf einen finanziellen Gewinn ab. Der Begriff wird aber häufig für beide Phänomene benutzt.

Was raten Sie: Was sollte man tun oder nicht tun, wenn man eine Sextortion-Email erhält?
In jedem Fall sollten die Leidtragenden Anzeige bei der Polizei erstatten - auch wenn man zunächst aus Scham verunsichert ist. Auch von Zahlungen sollten die Opfer Abstand halten. Am besten ist es nicht auf die E-Mails zu reagieren und einen Screenshot anzufertigen. Zur Sicherheit empfiehlt es sich die Nachrichten nicht zu löschen, sondern im E-Mail-Postfach abzulegen.

Sextortion, Neue Gefahren für Unternehmen

„WACH AUF, datenschutz@mms-law.de! Ich kann sehen, was du tust, Pädo“ schreibt „Donald Lohmeier“, der uns nicht persönlich bekannt ist. Der besagte Herr „Lohmeier“ droht damit, die Datenschutz-E-Mail-Adresse unserer Kanzlei in Verbindung mit Sexfilmen im Internet zu veröffentlichen und „an alle Freunde und Verwandte“ zu schicken, wenn nicht sofort seine Bitcoin-Adresse „mit 5.000 € finanziert“ wird. Ob „Datenschutz“ Freunde und Verwandte hat, bezweifle ich - mit einem Schmunzeln. Sicher ist aber, dass Sextortion-Angriffe immer häufiger Unternehmen oder Freiberufler treffen. Die Angriffe reichen von praktisch bedeutungslosen Spam bis hin zu Attacken, die von organisierter Kriminalität zeugen. Gerade letztere stellen eine neue, ernste Bedrohung dar.

Sextortion-Angriffe können Opfer privat bzw. ohne Bezug zu Unternehmen betreffen, um diese zu Zahlungen zu erpressen. Die Angriffe werden aber immer raffinierter und nehmen zunehmend den Mittelstand ins Fadenkreuz. Das Opfer, als Mitarbeiter eines Unternehmens, ist dabei nur das „Werkzeug“ des Täters. Es liegt in der Natur der Sache, dass mit Sextortion-Angriffen besonders leicht Druck aufgebaut werden kann, um Opfer zu einer Handlung, Duldung oder pflichtwidrigen Unterlassung zu nötigen. Wer möchte schon, dass alle Kunden oder Kollegen die eigenen Nacktbilder per E-Mail erhalten!?

Unternehmen sind verpflichtet, eine Unternehmensorganisation zu schaffen, die darauf ausgerichtet ist, gesetzeskonformes Verhalten zu gewährleisten (sogenannte Compliance). So verurteilte das Landgericht München I (Urteil v. 10.12.2013 - 5 HKO 1387/10) ein Siemens-Vorstandsmitglied auf Schadenersatz in Höhe von 15 Mio. Euro wegen eines unzureichenden Compliance-Systems. Verantwortung muss aber nicht nur für „schwarze Kassen“, sondern auch für die Buchhaltung, Know-hows, Geschäftsgeheimnisse oder Kundenverträge, und eben IT-Sicherheit, Datenschutz und Reputationsschutz übernommen werden.

Dr. Marc Maisch |
Maisch Mangold Schwartz Anwälte

Herr Rechtsanwalt Dr. Marc Maisch berät bundesweit zu allen Fragen des Internet- und Datenschutz- und Vertragsrechts. Neben Unternehmen gehören auch Sportverbände, Social-Media-Agenturen, IT-Dienstleister, Behörden und Privatpersonen zu seinen Mandanten. Er ist auch als externer betrieblicher Datenschutzbeauftragter (TÜV Nord) tätig. Als Mitglied von Blackstone432.de hält er deutschlandweit Keynotes und Vorträge u.a. über Identitätsdiebstahl und Internetrecht und schreibt gerade an einem Buch zu Cloud Computing nach der Datenschutzgrundverordnung (O'REILLY).

www.mms-law.de
Tel.: 089 265675
www.facebook.com/socialmediaanwalt/

Gerade hier können sich Sextortion-Angriffe auswirken:

• Vermögenswerte sind dann zumindest mittelbar gefährdet, wenn das Opfer rechtlich oder faktisch in der Lage ist, Zahlungen des Unternehmens an Dritte zu veranlassen. Möglich ist auch, dass der Täter die Herausgabe von (Admin-)Passwörtern oder Unternehmensinterna fordert, um einen großangelegten CEO-Fraud vorzubereiten. Beim CEO-Fraud (dt. Betrug) gibt sich der Täter mittels interner Informationen, gefälschter E-Mail-Adressen oder, wie in dem am 3. September 2019 von Forbes berichteten Fall, mit immitierter Stimme gegenüber der Buchhaltung, als der Geschäftsführer aus, der eine Zahlung anweist. Auf diese Weise hat ein britisches Unternehmen € 220.000 an einen unbekannten Täter verloren.

• Nicht weniger gefährlich sind Angriffe auf das Know-How. Seit Inkrafttreten des neuen Geschäftsgeheimnisgesetz am 26. April 2019 können Geheimnisse nicht mehr allein wegen der Entscheidung des Geheimnisinhabers geschützt werden. Überhaupt liegt ein Geschäftsgeheimnis erst dann (gem. § 2 Nr. 1 b GeschGehG) vor, wenn der rechtmäßige Geheimnisinhaber „angemessene Geheimhaltungsmaßnahmen“ getroffen hat. Darunter sind - analog Art. 32 DSGVO - technische und organisatorische Schutzmaßnahmen zu verstehen. verstehen.

• Auch das neue Datenschutzrecht zwingt Unternehmen dazu, ein angemessenes Datenschutzniveau, insbesondere den Schutz der Vertraulichkeit von personenbezogenen Daten (s. Art. 32 Abs. 1, lit. b DSGVO) sicherzustellen. Ganz gleich, ob es sich um Kundendaten oder Beschäftigtendaten handelt. Die Geschäftsleitung treffen strenge Rechenschaftspflichten gem. Art. 5 Abs. 2 DSGVO, dass Daten DSGVO-konform verarbeitet werden. Fehler in diesem Bereich können zudem Schadenersatzklagen nach sich ziehen, bei denen sich Unternehmen nur dann exkulpieren können, wenn sie nachweisen können, die DSGVO hinreichend eingehalten zu haben.

Es gibt nicht den Sextortion-Angriff aus dem Schulbuch. Sextortion-Angriffe rangieren von Spam bis hin zur gezielten Manipulation von Menschen. Strategische, organisatorische und technische Maßnahmen können helfen, das Schadenseintrittsrisiko auf ein vertretbares Maß zu senken. Im Rahmen einer Bewertung sollte geprüft werden, welches Vermögen und welche Geschäftsbereiche besonders durch ein Fehlverhalten eines Mitarbeiters gefährdet sind. Können. Admin-Passwörter ausgelesen oder von einem Administrator allein geändert werden? Welche Prozesse sichern Überweisungen ab? Wie werden neue oder geänderte Bankdaten überprüft? Gibt es ein Vier-Augen-Prinzip ab bestimmten Beträgen? Mitarbeiter sollten nicht nur auf die Gefahren, denen sie am Arbeitsplatz begegnen können, geschult werden - hier unterliegt der Arbeitgeber bereits einer arbeitsrechtlichen Fürsorgepflicht. Zum Schutz der IT-Compliance sollten ferner auch Empfehlungen für die Privatnutzung gegeben werden, insbesondere auch, wie man sich technisch besser schützen kann (Passwortmanager, Browser-Check, Umgang mit Social Media usw.).

Die Sicherstellung von Softwareupdates, Netzwerküberwachung, Malware-Detection, E-Mail-Verschlüsselung, regelmäßige Simulationen von Phishing- und Sextortion-Angriffen per E-Mail und hinreichende Wartung von Servern und IT-Endgeräten sorgen für technischen Rundumschutz. In jedem Fall rentiert sich die Bestellung eines internen oder externen betrieblichen Datenschutzbeauftragten, der die Geschäftsleitung bei allen Fragen des Datenschutzes, möglichst auch der IT-Compliance und Data Governance, beratend und unterstützend zur Seite steht. In diesem Sinne: Schützen Sie Ihr Unternehmen und bleiben Sie sicher!

Wie kann ich mich vor **Sextortion** schützen?

Vorsicht, ist besser als Nachsicht - eine altbewährte Regel, die gerade bei Sextortion von Vorteil ist. Cyberkriminelle verfahren bei Sextortion-Fällen nach einem einfachen Prinzip: Sie spielen mit der Angst, Scham und Unwissenheit ihrer Opfer. Und genau hier liegt der Schlüssel zur Lösung - das Wissen um die Vorgehensweise der Kriminellen schützt jeden davor, ein Opfer zu werden. Daher sollten sich Internetnutzer zwei Dinge immer vor Augen halten: Das eine ist die Sensibilität für Cyberkriminalität: Sextortion, Spear Phishing, Trojaner - die Gefahr "surft" immer mit. Hier sollte stets eine gewisse Portion Misstrauen mitgebracht werden. Ein zweiter wesentlicher Faktor, der vor kostspieligen Erfahrungen schützt, ist das Wissen um die Angriffsmethoden bei Sextortion.

Vier Ereignisse, die Sextortion begünstigen:

1. Selbst versandtes, pikantes Bildmaterial
2. Versehentlich heruntergeladene Schadsoftware
3. Gehackte Online-Speicherdienste
4. Reinfall auf Betrugs-E-Mails

1. Selbst versandtes pikantes Bildmaterial

Die erste Regel lautet "Jeder ist seines Glückes Schmied": Versenden Sie niemals bloßstellende Bilder oder Videos von sich selbst! Ganz egal, wer der Empfänger ist oder zu sein vorgibt. Alles was über das Internet geteilt wird, kann auch veröffentlicht werden. Täter können selbst Video-Chats aufzeichnen und anschließend ins Netz stellen. Speziell von Geräten, die Sie für Ihre Arbeit nutzen, sollten keine pikanten Bilder versendet werden. Führungskräfte in Unternehmen sind attraktive Ziele für Kriminelle, da die geforderte Summe noch höher angesetzt werden kann.

Richard Renner | Perseus Technologies GmbH

Richard Renner ist Geschäftsführer der Perseus Technologies GmbH, hat mehr als 18 Jahre Erfahrung in den Bereichen Versicherungen, Risikomanagement und Cybersicherheit. Zuvor war er u. a. bei Aon Risk Solutions Deutschland und bei der FinLeap GmbH tätig.

www.perseus.de

2. Versehentlich heruntergeladene Schadsoftware

Wenn Sie Schadsoftware heruntergeladen haben, kann es passieren, dass Dritte auf Ihre Endgeräte (Smartphone, Computer, Tablet etc.) zugreifen. Besondere Vorsicht gilt hier wieder bei Dienstgeräten - nicht zuletzt um unangenehme Gespräche mit Ihren Kollegen und Vorgesetzten zu vermeiden.

- Um Malware-Angriffe zu vermeiden, sollten Sie regelmäßig Sicherheitsupdates installieren und auf eine über den Standart hinausgehende Antivirenprogramme installieren.
- Vorsicht vor Phishing-E-Mails! Sobald Sie gebeten werden Daten, wie zum Beispiel den Login, einzugeben, sollten Sie Absender, weiterführende Links und ähnliches genau prüfen. Öffnen Sie keine Anhänge oder Links von verdächtigen Absendern.

- Überlegen Sie sich gut, welche Internetseiten Sie besuchen und prüfen Sie, ob diese vertrauenswürdig sind. Mittlerweile ist es schon möglich, sich durch den bloßen Besuch einer Webseite mit einem Schadprogramm zu infizieren.

- Schalten Sie außerdem Ihre elektronischen Geräte und Ihre Webkamera ab, wenn Sie diese nicht benutzen und nutzen Sie einen Kamera-Sichtschutz.

Tipp: *Nutzer von Perseus.de erhalten einen dauerhaften Schutz mit unserem integrierten Browser-Check und mit unserer intelligenten Sicherheitssoftware, die effektiv vor Sextortion durch. Malware-Angriffe schützt. Zudem werden Unternehmer und ihre Mitarbeiter mit regelmäßigen Phishing-Tests nachhaltig für Cybergefahren sensibilisiert, um erfolgreiche Angriffe zu verhindern.*

3. Gehackte Online-Speicherdienste

Seien Sie besonders gründliche bei der Auswahl Ihres Online-Speicherdienstes! Prüfen Sie welche Sicherheitsmaßnahmen vom Anbieter getroffen wurden, welche Erfahrungen andere Nutzer gemacht haben, ob es bereits Sicherheitsvorfälle gab und wie mit diesen verfahren wurde.

Tipp: *Verwenden Sie ein sicheres Passwort, das möglichst lange (mind. acht Zeichen), schwer zu erraten ist und sich aus einer Kombination von Zahlen, Klein-/ Großbuchstaben und Sonderzeichen zusammensetzt.*

4. Reinfall auf Betrugs-E-Mails

In den meisten Sextortion-Fällen erfolgt der Betrug per E-Mail. Die Empfänger haben in diesen Fällen oft nichts zu befürchten. Bei diesen E-Mails handelt es sich meist um leere Drohungen. Der Angreifer besitzt kein belastendes Material und hofft darauf, dass der Empfänger in letzter Zeit pornographische Inhalte konsumiert oder pikante Dateien versendet hat und aus Angst der Zahlungsaufforderung nachkommt. Als Druckmittel nennt der Täter häufig Passwörter, die gegebenenfalls während eines fruheren Daten-Vorfalls bekannt wurden. Es gibt auch Fälle bei denen eine Seite genannt wird, auf welcher das Opfer unterwegs war.

- Nutzen Sie sichere Passwörter sowie eine Zwei-Faktor-Authentifizierung und prüfen Sie, ob Ihre Kontodaten online einsehbar sind. Falls Sie eine Sextortion-Nachricht erhalten haben, ändern Sie umgehend Ihr Passwort! Bei dieser Methode sind Sie üblicherweise nicht das einzige Opfer des Täters. Die E-Mails gehen an eine größere Personengruppe. Eine Internetsuche nach ähnlichen Fällen gibt oft Aufschluss über aktuelle Sextortion-Wellen.

Tipp: *Perseus bringt Ihnen und Ihren Mitarbeitern einen selbstbewussten Umgang mit Cybersicherheit bei, mit einem Online-Training und regelmäßigen Phishing-Simulationstest.*

Für alle vier Sextortion-Formen gilt

1. Reagieren Sie auf keinen Fall auf die Nachricht
2. Gehen Sie nicht auf die Zahlungsaufforderung ein
3. Erstatten Sie umgehend Anzeige der Polizei.
4. Im Falle einer Veröffentlichung wenden Sie sich zudem an das soziale Medium auf welchem die Bilder ersichtlich sind, sodass dieses sie schnellstmöglich von der Seite nehmen kann.

Wir kümmern uns um Ihre **Cybersicherheit**, Sie sich um Ihre Geschäfte.

Perseus 360° Cybersicherheitspaket abschließen und Bußgelder, Betriebsunterbrechungen und Reputationsschäden vermeiden!

Unsere Angebote

Start

Individuell vorsorgen:

Perfekt für Unternehmer, die kostenlos und schnell die Grundlagen der Cybersicherheit und des Datenschutzes erlernen möchten. Online, zu jeder Zeit und an jedem Ort.

Pro

Ganzheitlich schützen

Cybersicherheit als Komplettservice: Perfekt für kleine und mittlere Unternehmen, die eine einfache, günstige und umfassende Cybersicherheits- und Datenschutzlösung suchen.

Premium

Zusätzlich absichern

Perfekt für Unternehmen, die mit einer zusätz-lichen Kostenabsicherung ihr Cyberrisiko mini- mieren wollen - der Komplettservice mit Kosten-Airbag.

Alle Funktionen	Start	Pro	Premium
Online-Sicherheitstraining	✓	✓	✓
24h/7 telefonische Notfallhilfe	✗	✓	✓
Simulierte Phishing-E-Mails	✗	✓	✓
Cybersicherheits-Führerschein	✗	✓	✓
Datenschutz-Führerschein	✗	✓	✓
IT-Sicherheitsprüfung	✗	✓	✓
Cybersicherheitsübersicht für Ihr Unternehmen	✗	✓	✓
Kundenservice Hotline	✓	✓	✓
Malware-Scanner	✗	✓	✓
Browser-Check	✓	✓	✓
Passwort-Generator	✓	✓	✓
Datensicherheits-Check	✗	✓	✓
Angriffsalarm	✗	✓	✓
Cyber-Schutzbrief			
IT-Forensik-Experten vor Ort	✗	✗	✓
Datenwiederherstellung und Entfernung der Schadsoftware	✗	✗	✓
Systemverbesserung nach Angriff (bis zu 10.000 €)	✗	✗	✓
Prüfung datenschutzrechtlicher Informationspflichten (bis zu 2.000 €)	✗	✗	✓

Über **Perseus**

Perseus bietet Unternehmen einen 360-Grad-Service für Cyber-Sicherheit und Datenschutz an. Ziel von Perseus ist die Etablierung einer langfristigen Sicherheitskultur zur Prävention, Abwehr und finanziellen Absicherung gegen Cyber-Kriminalität. Die Leistungen umfassen u.a. regelmäßige Phishing-Simulationstests, browserbasierte Mitarbeitertrainings, eine 24/7-Cyber-Notfallhilfe und eine intelligente Antivirensoftware.

Das Berliner Unternehmen gehört mit seinen über 30 Mitarbeiterinnen und Mitarbeitern zur finleap-Gruppe und sitzt im Fintech Hub “H:32”, Europas größten Hub für Fintech-Unternehmen. Der Unternehmensname lehnt sich an die Legende des Perseus an. Dieser Held der griechischen Mythologie steht für Schutz und Sicherheit.

Noch weitere Fragen?

Vereinbaren Sie einen unverbindlichen Beratungstermin mit unserem Kundenservice:

Hardenbergstr. 32, 10623 Berlin
Telefon: **030/95 999 80 80** (Mo - Fr 09:00-18:00 Uhr)
E-Mail: **info@perseus.de**

www.perseus.de

perseus.
Cybersicherheit auf den Punkt