Firewall.Spam.Junk.Würmer.Hacker.Virus. Phishing.Trojaner

SiCHERES_INTERNET

Eine Präventionskampagne des Polizeipräsidums Oberfranken

IHRE OBERFRÄNKISCHE POLIZEI INFORMIERT

Das WWW (world wide web), so wie wir es heute kennen, existiert erst seit 1991. Die Möglichkeit eines Datenaustausches über Telefonleitung gab es jedoch schon viele Jahre vorher. Im Jahr 1988 jagte der erste Virus mit dem Namen „Internet Worm“ durch die Verbindungen.

Somit gab es bereits kriminelle Aktivitäten, als das Internet noch in den Kinderschuhen steckte.

Mit dieser Broschüre wollen wir aufklären und beraten.

Auf den folgenden Seiten beschreiben wir, wie Sie die Gefahren des Internets erkennen und sich davor schützen können.

SiCHERES INTERNET?

Computerkriminalität

Immer mehr Haushalte in Deutschland besitzen PCs. Die Bürgerinnen und Bürger kommunizieren mittlerweile wie selbstverständlich über das Internet miteinander. Auch in Firmen und Behörden ist ein Arbeiten ohne ständige Nutzung der Informations- und Kommunikationstechnik nicht mehr vorstellbar. Das Internet boomt und ist heute aus der Medienlandschaft nicht mehr wegzudenken. Allein in Deutschland nutzten schon Ende 2000 mehr als 20 Mio. Menschen das Internet. Die unüberschaubare Vielfalt der mehr als 210 Mio. Online-Angebote weltweit birgt neben den unbestreitbaren Chancen und Nutzungsmöglichkeiten im Dienstleistungs- und Bildungsbereich zugleich erhebliche Gefahren und Risiken.

Einige Kriminalitätsformen wurden durch die Computertechnik überhaupt erst möglich. Zu nennen sind hier beispielhaft das Ausspähen von Daten, die Datenveränderung, die Computersabotage oder der Computerbetrug. Andere konventionelle Kriminalitätsformen wurden aus der analogen in die digitale Welt überführt. Hierunter fallen insbesondere die Verbreitung von Kinderpornografie, die Streuung gewaltverherrlichenden und extremistischen Gedankenguts, der Vertrieb von Drogen und verschreibungspflichtigen Arzneimitteln oder bestimmte Formen der Wirtschaftskriminalität.

Bis zum Jahre 1986 waren die Möglichkeiten, der Computerkriminalität mit den Mitteln des Strafrechts zu begegnen, sehr eingeschränkt. Durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986 hat der Gesetzgeber diesen Zustand weitestgehend beseitigt.

Für kriminelle Handlungen bei der Nutzung von Datenverarbeitungsanlagen sieht das **Strafgesetzbuch** folgende Straftatbestände vor:

- Ausspähen von Daten
- Computerbetrug
- Fälschung und Unterdrückung beweiserheblicher Daten
- Datenveränderung
- Computersabotage

Das **Urheberrechtsgesetz** findet Anwendung bei der Herstellung von Raubkopien.

Computerkriminalität

Viren (aus dem lateinischen virus = das Gift)

Viren sind eine Art böswillige Software mit dem Merkmal der Selbstreproduktion. Sie können in Ihrem gesamten Computersystem einschließlich Speichermedien große Schäden anrichten. Wenn ein Virus keine besonders schädigende Funktion aufweist, so könnte er trotzdem die Abwehrfunktion und die Leistung Ihres Systems schwächen.

Die früheren Erkenntnisse, dass Viren nur nach Öffnen einer infizierten Datei aktiv werden, sind überholt. Vielmehr ist zwischenzeitlich auf Grund der Virenvielfalt jegliche unkontrollierbare und systemschädigende Ausbreitung möglich.

Virenvielfalt - Kombinationen
Die Vielfalt an Computerviren macht eine genaue Klassifizierung oft nur schwer möglich. Immer häufiger treten folgende Viren-Kombinationen auf:

Datei-Viren
befallen ausführbare Programme, deren Dateinamen in der Regel mit ".exe" oder ".com" enden. Betroffen davon sind vor allem Text- und andere installierte Anwendungsprogramme. Beim Start des zunächst infizierten Programms wird das Virus automatisch mit ausgeführt und befällt andere Programme.
Die Infizierung läuft beispielsweise über einen E-Mail-Anhang, eine Diskette, CD-ROM, USB-Sticks, Speicherkarten, DVD oder externe Festplatten.

Makroviren
verstecken sich in Word- oder Excel-Dokumenten. Grundsätzlich automatisieren Makros die Arbeitsabläufe. Virenverseuchte Dokumente können nach dem Befall einerseits eine einfache Scherzprogrammierung enthalten und andererseits die Löschung des Dokumentes zur Folge haben.

Bootsektor-Viren
verbreiten sich vorwiegend über Disketten. Bei jedem Systemstart wird das Virus aktiv, befällt die Bootsektoren oder infiziert eingelegte Disketten. Bösartige Varianten löschen die Festplatte

Tipps

» Antivirensoftware installieren und aktualisieren (www.antivir.de)

» Regelmäßige Updates Ihres Betriebssystems durchführen

» Firewall installieren

» E-Mails mit unbekannter Herkunft nicht öffnen

Viren,Würmer&Trojaner

Wie kann man Viren erkennen?

- Oft verraten sich Viren durch eine leere Betreffzeile oder der Betreff macht den Adressaten neugierig.
- Viele Viren haben einen englischsprachigen Text in der Betreffzeile. Erhalten Sie solche E-Mails unaufgefordert, sollten Sie diese sofort löschen.
- Da vor allem Unternehmen und Behörden E-Mails filtern, ist es empfehlenswert, wichtige Nachrichten ausschließlich im Texfeld zu schreiben. Vermeiden Sie Anhänge.
- Gefährliche Virenprogramme sind immer "angehängt".
- Seien Sie besonders kritisch bei Programm-Dateien mit den Endungen .exe, .bat, .com oder .vbs.
- Damit Sie den Dateityp sehen und erkennen können, sollten Sie die Standardkonfiguration ihres Rechners ändern: Entfernen Sie im Windows-Explorer unter Extras/Ordneroptionen/Ansicht/Erweiterte Einstellungen/Dateien und Ordner das Häkchen vor "Erweiterungen bei bekannten Dateitypen ausblenden".
- Stellen Sie die Sicherheitseinstellungen Ihres E-Mail-Programms so ein, dass kein Script automatisch ausgeführt wird.
- Führen Sie generell keine aus unsicherer Quelle oder per E-Mail zugesandten Anhänge aus.

Was tun bei Virenbefall?

Beenden Sie sofort die Arbeit am PC und sichern Sie wichtige Daten.

Wie schützen vor Viren?

Jeder Anwender sollte auf seinem Rechner einen Virenscanner installiert haben, der ständige Aktualisierungen durchführt. Trotzdem ist ein 100-prozentiger Schutz wegen der rasanten Entwicklung auf der Datenautobahn nahezu unmöglich.
Prüfen (scannen) Sie Datenträger vor der Verwendung immer mit Ihrem Virenscanner.

Strafbarkeit nach dem Strafgesetzbuch (StGB)

Wer ein Virus erstellt oder verbreitet, könnte damit eine Datenveränderung oder eine Computersabotage begangen haben.

Schadensersatzansprüche nach dem Bürgerlichen Gesetzbuch (BGB)

In Verbindung mit den obigen Strafvorschriften bestehen auch zivilrechtlicher Schadensersatz-, Beseitigungs- und Unterlassungsanspruch.

Viren,Würmer&Trojaner

„Trojanische Pferde“

Eine besonders „heimtückische“ Sonderform von Viren sind so genannte „Trojanische Pferde“.

Dies sind in aller Regel harmlose und brauchbare Programme, die allerdings mit einem Virus, einem Wurm oder einer Spionagesoftware infiziert wurden. Die infizierten Programme beinhalten nach dem Befall eine äußerst schädliche Funktion für den Anwender. Diese im Hintergrund und unbemerkt ablaufende Funktion ermöglicht es Unberechtigten, gezielt persönliche Daten auszuspähen. So gelangen diese Straftäter in den Besitz von sensiblen persönlichen Daten wie Passwörter oder Zugangs- und Kreditkartennummern.
Wird das Programm installiert, kann es oft Monate dauern, bis ein Anwender dieses schädliche Programm auf seinem System bemerkt.

Hoaxes

Bei einem Hoax handelt es sich um keinen Virus, sondern lediglich um eine als oftmals böswilligen Scherz versandte Falschmeldung. Sie gaukelt dem PC-Benutzer vor, ihn beispielsweise über einen gefährlichen Virus zu informieren und zu warnen. So werden Anwender etwa dazu aufgefordert, zur Virenabwehr bestimmte (wichtige) Dateien zu löschen. Ergänzt wird die Meldung oftmals mit dem Rat, die warnende E-Mail an Freunde und Bekannte weiterzuleiten. Einziger Sinn und Zweck dieser Hoaxes ist es, Anwender zu verunsichern und Panik zu verbreiten.

Wirksamer Schutz vor Trojanern

Das besondere Problem bei Trojanern ist, dass es sich auf den ersten Blick immer um ein anscheinend nützliches Programm handelt. Man ist in aller Regel darauf angewiesen, dass irgendwann jemand die verborgene Schadensfunktion entdeckt.

Ab diesem Zeitpunkt sollte der Name des Trojaners in das Virenschutzprogramm eingetragen werden. Erst dann tritt ein Schutzmechanismus gegen diesen Trojaner in Kraft.

Während Online-Sitzungen gelingt es oftmals, mittels aktivierten „Anti-Trojaner-Programmen“ eine Infizierung zu verhindern.

Ist mein PC schon infiziert?

Ob sich auf dem eigenen PC bereits ein „Trojanisches Pferd“ befindet, kann anhand verschiedener Veränderungen erkannt werden.

» Wird Windows einfach während einer Sitzung beendet oder heruntergefahren,
» ist die Taskleiste plötzlich nicht mehr sichtbar,
» sind die Maustasten plötzlich vertauscht,
» verändern sich die Farben des Systems,
» schließt sich das CD-Laufwerk von allein,
» finden während einer Online-Sitzung plötzlich ungewollte Übertragungen statt,

dann besteht der dringende Verdacht einer Trojaner-Infektion.

Grundsätzlich gelten hier die selben Schutzhinweise wie bei Viren.

Viren,Würmer&Trojaner

Softwarepiraterie

Die Hersteller von Software versuchen mit großem Aufwand ihre Produkte gegen die Vervielfältigung durch einfaches Kopieren zu schützen. Dies geschieht beispielsweise durch den Einbau von Seriennummernabfragen.

Der **Software-Pirat** erwirbt ein Original oder eine Kopie (gegebenenfalls ganz legal) der zu vervielfältigenden Software, kopiert diese beliebig oft und veräußert diese Kopien. Durch Softwarepiraterie entstehen der Wirtschaft enorme Schäden.

Professionelle Raubkopierer erstellen hierbei Datenträger, die für den Laien mitunter nicht mehr als Fälschung erkannt werden können. Das Wort **Raubkopie** bezeichnet eine illegale Kopie eines urheberrechtlich geschützten Werkes. Dabei unterbleibt die Bezahlung an den Urheber oder den Rechteinhaber. Nach dem Urheberrecht wird als Raubkopie eine unrechtmäßig erstellte Kopie von Daten bezeichnet. Dabei kann es sich beispielsweise um Filme, Musikstücke, E-Books, Computerprogramme oder komplette Datenbanken handeln.

Das Anfertigen und Verbreiten von unautorisierten Kopien ist in fast allen Ländern der Welt gesetzlich verboten.

Da Raubkopierer nichts entwenden sondern lediglich kopieren, fehlt den Tätern oftmals das Unrechtsbewusstsein. Dies schützt jedoch nicht vor Strafe.

Der Gesetzgeber droht für diese Urheberrechtsverletzung Freiheitsstrafen von bis zu fünf Jahren an.

Auch der Kauf von Raubkopien ist rechtswidriges Verhalten.

Schützen Sie sich!

» Nutzen und kaufen Sie ausschließlich originale Software und Musiktitel

» Meiden Sie Tauschbörsen

» Kaufen Sie bei Online-Auktionshäusern keine verbilligte Software

» Achten sie auf Markenzertifikate

Softwarepiraterie

Wirtschaftskriminalität
ist die Bezeichnung für Straftaten, die im Rahmen tatsächlicher oder vorgetäuschter wirtschaftlicher Betätigung begangen werden und über eine Schädigung von Einzelnen hinaus das Wirtschafsleben beeinträchtigen oder die Allgemeinheit schädigen können.
Darunter fallen beispielsweise Betrugsdelikte im Zusammenhang mit **E-Commerce** und Kapitalanlagen, bestimmte Erscheinungsformen der organisierten Kriminalität, Konkursdelikte und Korruption.

Betrugsarten im Zusammenhang mit Datenverarbeitungssystemen werden als **Computerkriminalität** bezeichnet.

Dazu gehören insbesondere Straftaten wie

- Betrug mittels rechtswidrig erlangter unbarer Zahlungsmittel
- Computerbetrug
- Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten
- Fälschung beweiserheblicher Daten
- Datenveränderung, Computersabotage
- Ausspähen von Daten
- Software-Piraterie (private Anwender)
- Gewerbliche Software-Piraterie

„Sicherheit ist kein Pokerspiel“

Seien Sie misstrauisch und informieren Sie sich:

Kriminalpolizeiliche Beratungsstellen in Oberfranken
www.polizei-oberfranken.de/schuetzenvorbeugen/beratung/adressen/index.html/725

Bundesamt für Sicherheit in der Informationstechnik
www.bsi-fuer-buerger.de

www.polizei-beratung.de

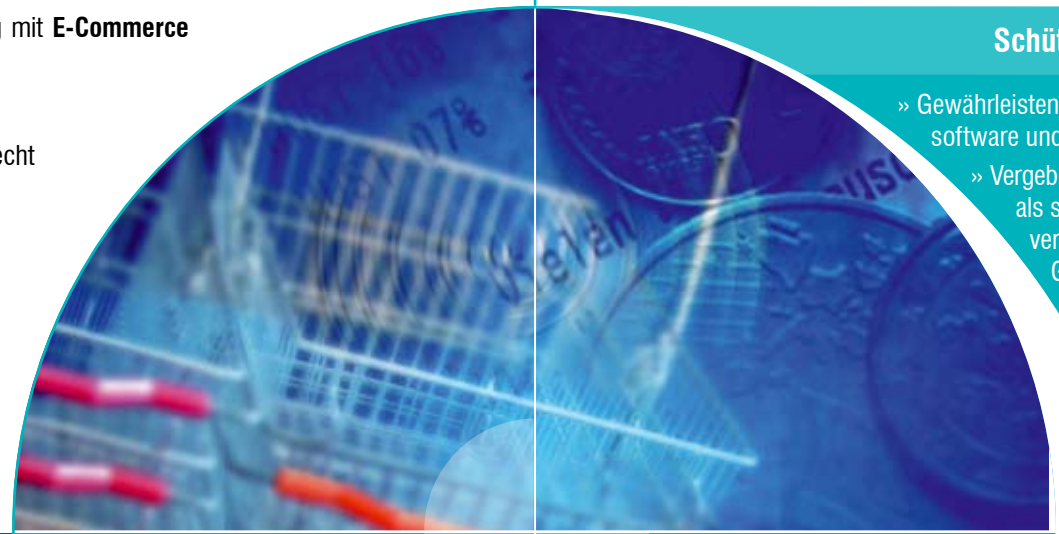
Wirtschaftskriminalität

E-Commerce (Geschäftsabwicklung via Internet)

Im Internet werden täglich millionenfach Waren gekauft und verkauft. Dies geschieht vorwiegend in Onlinekaufhäusern, Onlineauktionshäusern oder in Foren. Längst nutzen auch Kriminelle den weltweiten Handel von Waren und Dienstleistungen im Internet.
Zu sorglos gehen Nutzer oftmals bei Online-Geschäften mit persönlichen Daten um und öffnen so den Kriminellen vielfach „Tür und Tor“.

Welche rechtswidrige Handlungen werden im Zusammenhang mit **E-Commerce** begangen?

- Betrugsdelikte in Verbindung mit Zahlungsvorgängen
- Verstöße gegen das Urheber-, Marken- und Wettbewerbsrecht
- Fälschungsdelikte
- Verstöße gegen das Arzneimittelgesetz
- Verbreitung von Pornografie
- Anbieten verbotener Dienstleistungen und Waren
- Hehlerei



e-Commerce

Gefahren für Unternehmen

- Computer-Sabotage (Attacken gegen Unternehmensrechner)
- Datenmanipulation
- Datenspionage
- Betrug

Schützen Sie sich!

» Gewährleisten Sie Basissicherheit durch Antivirensoftware und Firewall

» Vergeben Sie sichere Passwörter mit mehr als sechs Buchstaben und Ziffern und verwenden Sie dabei keine Namen oder Geburtsdaten

» Informieren Sie sich über den Verkäufer

» Lesen Sie Artikelbeschreibung und Vertragsvereinbarungen genau und vollständig durch

» Vergleichen Sie Preise

e-Banking

Die Vorteile des auch als Homebanking bezeichneten e-Bankings oder Online-Bankings liegen auf der Hand: Jederzeit direkte Erledigung aller Bank- und Finanzgeschäfte aus dem „Wohnzimmer“ bei kostengünstigen Optionen.

Wie sicher ist Online-Banking?

Beim T-Online-Verfahren erhält jeder Banking-Kunde eine Zugangsnummer für T-Online, ein dazugehöriges Passwort sowie eine Persönliche Identifikations-Nummer **(PIN)**. Ebenso wie bei der EC-Karten-Geheimnummer ist es unbedingt ratsam, die Daten keiner dritten Person weiterzugeben. Versucht ein Unbefugter über seinen T-Online-Anschluss und mit dem Wissen einer fremden Kontonummer, die PIN durch mehrmalige Eingabe zu erraten, sperrt der Rechner das Online-Konto bei der dritten Falscheingabe automatisch. Als weitere Sicherheitsbarriere werden bei jeder kontobelastenden Aktion des Kunden einmalige Transaktionsnummern **(TAN)** verwandt.

Damit ist das T-Online-Banking die derzeit sicherste Form, Bankgeschäfte direkt über die Datenautobahn zu tätigen.

Vorsicht bei Anfragen via E-Mail nach Ihren PIN und TAN. Ihre Bank wird Sie nie im Online-Verkehr dazu auffordern, diese personenbezogenen Daten mitzuteilen.

Nehmen Sie in diesem Fall sofort telefonisch mit Ihrer Bank Kontakt auf, denn es könnte sich bei der E-Mail um eine gefährliche „Phising-Mail“ handeln.

Achten Sie auf Ihre personenbezogenen Daten!

» Verwenden Sie stets aktuelle Virenschutzprogramme und eine Firewall

» Aktualisieren Sie ihr Systems regemäßig mit Sicherheitsupdates

» Wechseln Sie Passwörter und PIN regelmäßig

» Speichern Sie PIN und TAN nicht auf ihrem PC und bewahren Sie sie getrennt auf

Was sind "Dialer"? (englisch: to dial = wählen)

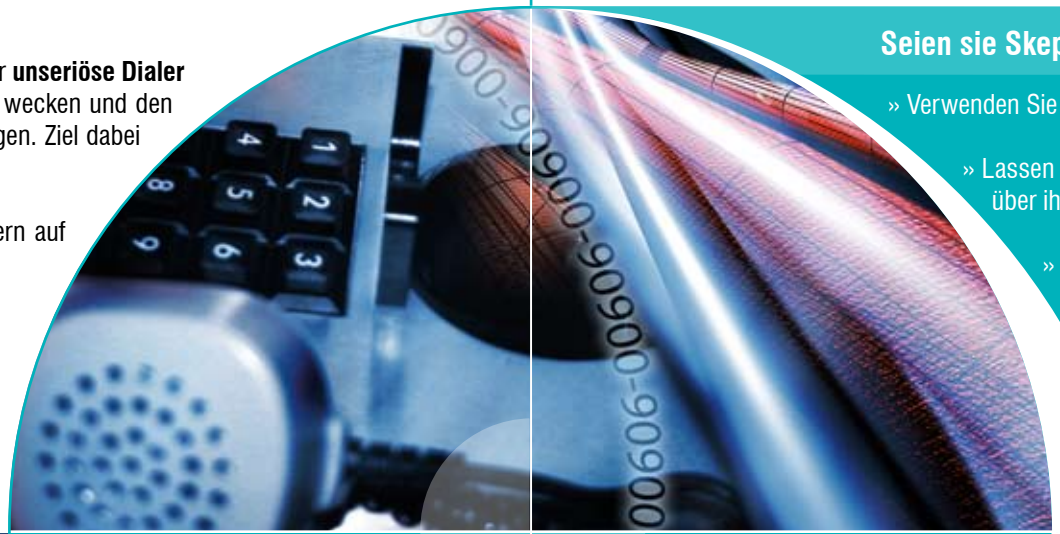
Dialer sind Internetprogramme, die einen PC über eine bestimmte Service-Nummer mit einem Internetserver verbinden. Um die hohen Nebenkosten der herkömmlichen Zahlungssysteme zu umgehen, entwickelten Softwareunternehmen diese Programme, die auf einem PC mit Internetanbindung installiert werden können und die Einwahl über kostenpflichtige Servicenummern ermöglichen. Die in Anspruch genommene Dienstleistung wird dabei mittels Telefonrechnung abgerechnet.
Dieses Abrechnungssystem nutzten im Besonderen die Erotik- und Pornobranche mittels der gebührenintensiven Einwahlnummern 0190 oder 0900.

Grundsätzlich unterscheiden sich zwei Typen von Dialern:

Der **seriöse Dialer** informiert über die entstehenden Kosten. Der **unseriöse Dialer** versucht durch Vortäuschen falscher Tatsachen, Neugierde zu wecken und den Nutzer zum Wählen der angebotenen Servicenummer zu bewegen. Ziel dabei ist es, die Kosten zu verschleiern.

Woran können Sie einen **unseriösen Dialer** für Servicenummern auf dem PC erkennen?

- Unbekannte Symbole in der Taskleiste
- Selbstständiges Einwählen des Modems in das Internet
- Plötzlich veränderte Startseite des Browsers
- Erscheinen einer 0190er Nummer im DFÜ-Netzwerk
- Automatisches Öffnen eines "Pop-up-Fenster" beim Start des Webbrowsers



Dialer

Woran können Sie ein unseriöses **Dialer-Programm** auf Ihrem PC erkennen?

- "exe."-Programm zum automatischen Download wird per E-Mail angeboten
- Gefälschte Absenderkennung zum Vortäuschen eines offiziellen Programmes oder einer offiziellen E-Mail
- Fehlender Kostenhinweis auf der angebotenen Internetseite des Downloads

Seien sie Skeptisch!

» Verwenden Sie eine aktuelle Firewall

» Lassen Sie 0910er und 0900er Nummern über ihren Telefondienstleister sperren

» Brechen Sie automatisch startende Downloads sofort ab

» Nutzen sie Dialer-Blocker

» Klären sie Mitnutzer auf

Strafbarkeit

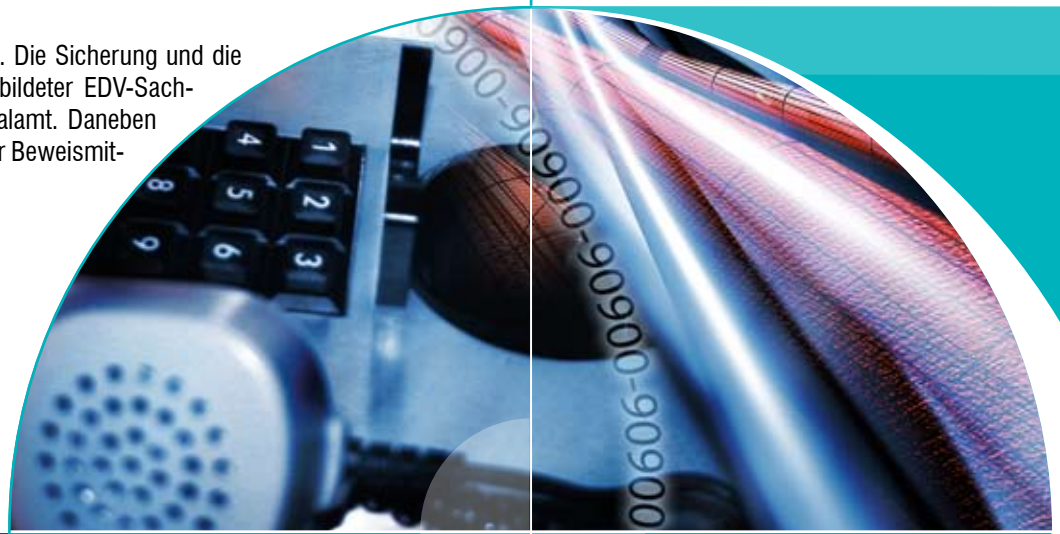
Waren die Angaben auf der Webseite zum Zeitpunkt eines Dateidownloads geeignet, den Nutzer über die tatsächlich anfallenden Gebühren oder über die Funktionsweise der Software zu täuschen, können bereits Anhaltspunkte für einen Coputerbetrug oder eine ebenfalls strafbare Datenveränderung vorliegen.

Beweismittel

Bei allen Straftaten können Beweismittel in digitaler Form anfallen. Die Sicherung und die Auswertung dieser EDV-Beweismittel ist Aufgabe speziell ausgebildeter EDV-Sachverständiger und Sachbearbeiter beim Bayerischen Landeskriminalamt. Daneben verfügen alle bayerischen Polizeipräsidien über regionale Stellen zur Beweismittelsicherung und Auswertung .

Damit die Polizei diese Straftaten umfassend aufklären kann, ist es grundsätzlich erforderlich,

- die Webseite des Anbieters und des Dateidownloads zu dokumentieren,
- die Funktionsweise der Dialer-Software zu überprüfen und
- den Empfänger der Anbietervergütung zu ermitteln.



Dialer

Pornografische Darstellung und sexueller Missbrauch von Kindern

Unter Kinderpornografie versteht man pornografische Darstellungen, die den sexuellen Missbrauch von unter 14-Jährigen zeigen.
Es ist unerheblich, ob die Darstellung ein reales Geschehen wiedergibt. So können auch Comics mit entsprechenden Darstellungen oder Erzählungen unter den Begriff "Kinderpornografie" den Tatbestand erfüllen.

Generell verboten ist die so genannte „harte Pornografie“, die sexuelle Gewalttätigkeiten, den sexuellen Missbrauch von Kindern oder sexuelle Handlungen von Menschen mit Tieren (Sodomie) zeigen. Im Falle der Kinderpornografie ist bereits der Besitz (Herunterladen auf den eigenen Rechner) strafbar.

Was unternimmt die Polizei?

Für die Sicherung und Auswertung dieser EDV-Beweismittel verfügen alle bayerischen Polizeipräsidien über regionale Stellen zur Beweismittelsicherung und Auswertung mit speziell ausgebildeten EDV-Sachverständigen.

Die Netzwerkfahndung beim Bayerischen Landeskriminalamt forscht ständig im Internet nach illegalen Angeboten und Inhalten.
Ihre nächste Polizeidienststelle nimmt jeden Hinweis, auf Wunsch auch vertraulich, entgegen.

Haben Sie Seiten mit kinderpornografischen Inhalten entdeckt?

» Nehmen Sie zeitnah Kontakt mit einer Polizeidienststelle auf und teilen Sie dies mit

Haben Sie irrtümlich kinderpornografische Bild- oder Videodateien herunter geladen?

» Verständigen Sie umgehend Ihre Polizeidienststelle, damit eine erfolgversprechende Beweissicherung durch speziell ausgebildete Polizeibeamte erfolgen kann.

Haben Sie unaufgefordert Kinderpornographie per E-Mail zugesandt bekommen?

» Leiten Sie diese E-Mail mit Anhang unverzüglich an die für Ihren Wohnsitz zuständigen Polizeidienststelle weiter.

Schutzmechanismen

» Beschränken Sie mit Filterprogrammen die Internetnutzung
» Surfen Sie mit Ihren Kindern gemeinsam
» Installieren Sie einen Viren-Scanner
» Setzen Sie eine Firewall ein
» Stimmen Sie zeitliche und inhaltliche Internetnutzung mit Ihren Kindern ab
» Sprechen Sie die Gefahren mit Ihren Kindern offen an
» Geben Sie keine persönlichen Daten bekannt
» Vermeiden Sie Online-Verabredungen

Weitere Infos:
http://www.bsi.de/

Kindgerechtes Internet

Chat

Für viele Kinder ist das Internet mittlerweile Teil des Alltags geworden. Sie surfen, spielen, chatten, mailen, recherchieren im Internet und informieren sich. Das weltumspannende Computernetz hat viel zu bieten: Unterhaltung und Spaß, Information und Bildung, Kommunikation und Interaktion. Doch neben den vielen Vorteilen, die das WWW bietet, können Kinder – da unterscheidet sich das Internet nicht von anderen Lebensbereichen - auch unangenehme Erfahrungen machen. Millionen von Einzelcomputern sind weltweit miteinander über Datenleitungen verbunden, unzählbare Unternehmen, Institutionen, Vereine, Privatpersonen stellen ihre Seiten ins Netz. Darunter sind auch Angebote, die für Kinder absolut ungeeignet sind. Leider reicht manchmal schon das Anklicken von Bannerwerbung, um Dinge zu sehen, die erschrecken oder nachhaltige Ängste hervorrufen.

Durch die Flüchtigkeit und scheinbare Anonymität der Kommunikation in Chat-Räumen entsteht der Eindruck, dass das Nutzen und Betreiben dieser Dienste faktisch keinen gesetzlichen Beschränkungen unterliegen. Ein Trugschluss: Grundsätzlich gelten auch in diesen Kommunikationsdiensten die gleichen Beschränkungen des Straf-, Jugend- und Medienrechts wie in anderen Internetdiensten und wie im realen Leben.

Oftmals gehen Kinder unbeaufsichtigt ins Netz, und die Erwachsenen sind sich der Gefahren oftmals nicht bewusst. Wer nicht selber chattet, hat kaum eine Vorstellung von beispielsweise CS-begeisterten Kindern (CS bedeutet Cybersex). Diese kindliche Neugier wiederum nutzen wesentlich ältere Personen schamlos aus.

So kann es zu verhängnisvollen Verabredungen kommen, denen ein Kind, viele Jugendliche und sogar manche Erwachsene nicht gewachsen sind.

Von besonderer strafrechtlicher Relevanz:
Kontaktanbahnung mit dem Ziel des sexuellen Missbrauchs

Der Gesetzgeber sieht bereits für diese Form eines Anbahnens von sexuellen Kontakten zu Kindern unter bestimmten Umständen eine erhebliche Freiheitsstrafe bis zu fünf Jahren vor.

Chat

Sexueller Missbrauch

Mehr als nur ein Randbereich im Internet sind die Verbreitung illegaler Inhalte, allen voran Pornografie und Gewaltdarstellungen. Sie stellen neben rechts- beziehungsweise linksextremistischen Online-Angeboten die größte Gefahr für Kinder und Jugendliche dar und nehmen deshalb alle Internetnutzer in die Pflicht.

Als pornografisch ist laut Bundesgerichtshof eine Darstellung anzusehen, „wenn sie unter Ausklammerung aller sonstigen menschlichen Bezüge sexuelle Vorgänge in grob aufdringlicher, anreißerischer Weise in den Vordergrund rückt und in ihrer Gesamttendenz ausschließlich oder überwiegend auf das lüsterne Interesse des Betrachters an sexuellen Dingen abzielt“.

Der Begriff des sexuellen Missbrauchs von Kindern umfasst in erster Linie Straftaten im Sinne der §§ 176 ff. des Strafgesetzbuches. Der Tatbestand ist dann schon erfüllt, wenn die Darstellung die Vornahme sexueller Handlungen eines Kindes an sich selbst zeigt und sich aus dem Zusammenhang der Aufnahme ergibt, dass es dazu von einem Dritten aufgefordert wurde.

Gewaltdarstellung

Das Internet schockiert auf vielen Seiten mit gewaltverherrlichenden Bildern oder Texten. Die oft menschenverachtenden Darstellungen oder Beschreibungen verletzen die Würde des Menschen.

» Melden Sie solche Inhalte Ihrer nächsten Polizeidienststelle

» Schützen Sie Ihr Kind

» Vermeiden Sie Kontakte mit gewaltverherrlichenden Videospielen

Handykriminalität - Handy Slapping

(englisch: fröhliches Draufschlagen)

Aktuell ist auf Schülerhandys eine vermehrte Zunahme von „Happy Slapping“ festzustellen. Hierbei wird mit einem Handy oder einer Videokamera ein Angriff auf einen Unbeteiligten gefilmt, wobei der Angreifer äußerst brutal auf das Opfer einschlägt. Die Filmaufnahmen veröffentlichen die Täter anschließend im Internet oder verbreiten sie per Mobiltelefon.

Ursprung dieser kriminellen Aktionen waren mehrere solcher Vorfälle im Jahr 2004 in England. In der Folgezeit berichteten auch vereinzelt Medien über Vorfälle auf dem europäischen Festland.

Handykriminalität

Seien sie wachsam!

» Melden sie rechtsrextreme und gewaltverherrlichende Videos auf Handys Ihrer Polizeidienstelle

Internet? Sicher!

Herausgeber Polizeipräsidium Oberfranken

Design Handwerkskammer Oberfranken

M. Müller, I. Reißenweber, M. Zimmer

Texte Polizeipräsidium Oberfranken
Sachgebiet Verbrechensbekämpfung

Redaktion Polizeipräsidium Oberfranken - Präsidialbüro

Für Ihre Notizen: