Polizei

SAARLAND
Großes entsteht immer im Kleinen.

Tatort Internet –
neue Gefahren durch die moderne Technik

Saarbrücken, 26.02.2021

Themen

- Was ist Cybercrime
- Datendiebstahl
- Das moderne trojanische Pferd
- Die ungewollte Verschlüsselung
- Betrug, Agenten und Liebe
- „Fleißige“ Support Mitarbeiter
- Schutzmaßnahmen

Was genau versteht man eigentlich unter Cybercrime?

Straftaten gegen

- **das Internet**
- **andere Datennetze**
- **Informationstechnische Systeme (IT-Systeme)**
- **Daten innerhalb von IT-Systemen**

Cybercrime umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden. (i.w.S.)

Bekämpfung von Cybercrime im Landespolizeipräsidium des Saarlandes

Wie begegnet das Saarland den neuen Herausforderungen?

Das Dezernat LPP 222 Cybercrime

Hauptaufgaben

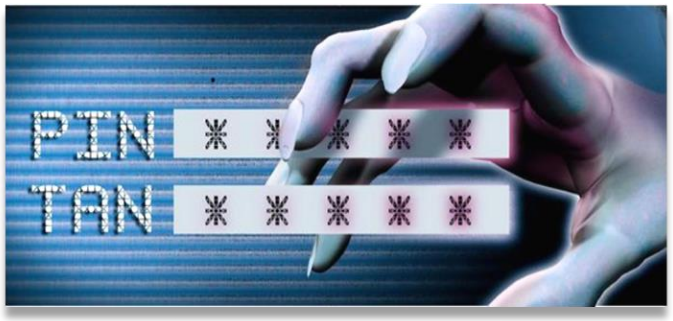
- „Computerkriminalität“(herausragende Fälle, hoher Schaden, neue/unbekannte Tatbegehungsweise, besonderer Sachverstand)
- Zentralstelle Cybercrime für das Saarland (Ansprechpartner für die Polizeidienststellen im Land und das BKA)
- ZAC – Zentrale Ansprechstelle Cybercrime (für Wirtschafts-unternehmen)

Personal LPP 222 Cybercrime

- 5 Beamte
- 3 Informatiker

Ausspähen von Daten

Wie gelangen die Kriminellen an unsere Daten und was fangen Sie damit an?



Phishing – Das Angeln nach Daten

Was ist Phishing?

Unter Phishing (Kunstwort aus **password** und **fishing**) versteht man den Versuch, mittels gefälschter Webseiten, E-Mails, Social Engineering, pp. an Daten des Opfers zu gelangen.

Typischer Ablauf:

1. Sie bekommen eine **E-Mail,** die **scheinbar von** Ihrer Hausbank, eBay, PayPal, usw. stammt
2. Inhalt: **Sie hätten ein Problem** („Transaktionsproblem“, „Ungewöhnliche Aktivitäten“, „Sicherheitsüberprüfung“, Konto zu lange inaktiv, etc.)
3. Sie werden **aufgefordert,** unbedingt einen **Link** in dieser E-Mail **anzuklicken**. Andernfalls gäbe es **ernsthafte Konsequenzen** (Konto- oder Accountsperrung, Kosten, pp.)
4. Sie klicken auf den Link
5. Es wird eine Webseite geöffnet, die wie Original-Webseite des Absenders aussieht
6. Sie geben dort für einen vorgetäuschten Datenabgleich viele persönliche Daten ein
7. Die eingegebenen Daten landen beim Täter

Typische Phishing E-Mail

amazon.com

27.11.2013

Wir brauchen Ihre Hilfe,

Wir benötigen ihre Hilfe damit es für sie weiterhin möglich ist ihr Amazon Konto wie gewohnt nutzen zu können.

Wo liegt das Problem?

Auf ihrem Amazon Kundenkonto wurde eine Bestellung getätigt welche auf eine nicht von ihnen angegebene Lieferadresse gesendet werden sollte.

Unser Sicherheitssystem hat diese Bestellung erkannt und storniert.
Wir bitten sie daher ihr Mitgliedskonto schnellstmöglich zu verifizieren um weiteren Komplikationen vorzubeugen.

Nach erfolgreicher Verifizierung können sie ihr Konto wieder im vollen Umfang nutzen.

Damit sie ihr Konto wieder uneingeschränkt nutzen können, verifizieren sie sich bitte durch Abgleich ihrer Daten als rechtmäßiger Besitzer.

Nach erfolgreicher Verifizierung können sie ihr Konto wieder im vollen Umfang nutzen.

Ihr Amazon Kundenservice

Was mache ich jetzt?

Nutzen Sie zur Verifizierung folgenden Link:

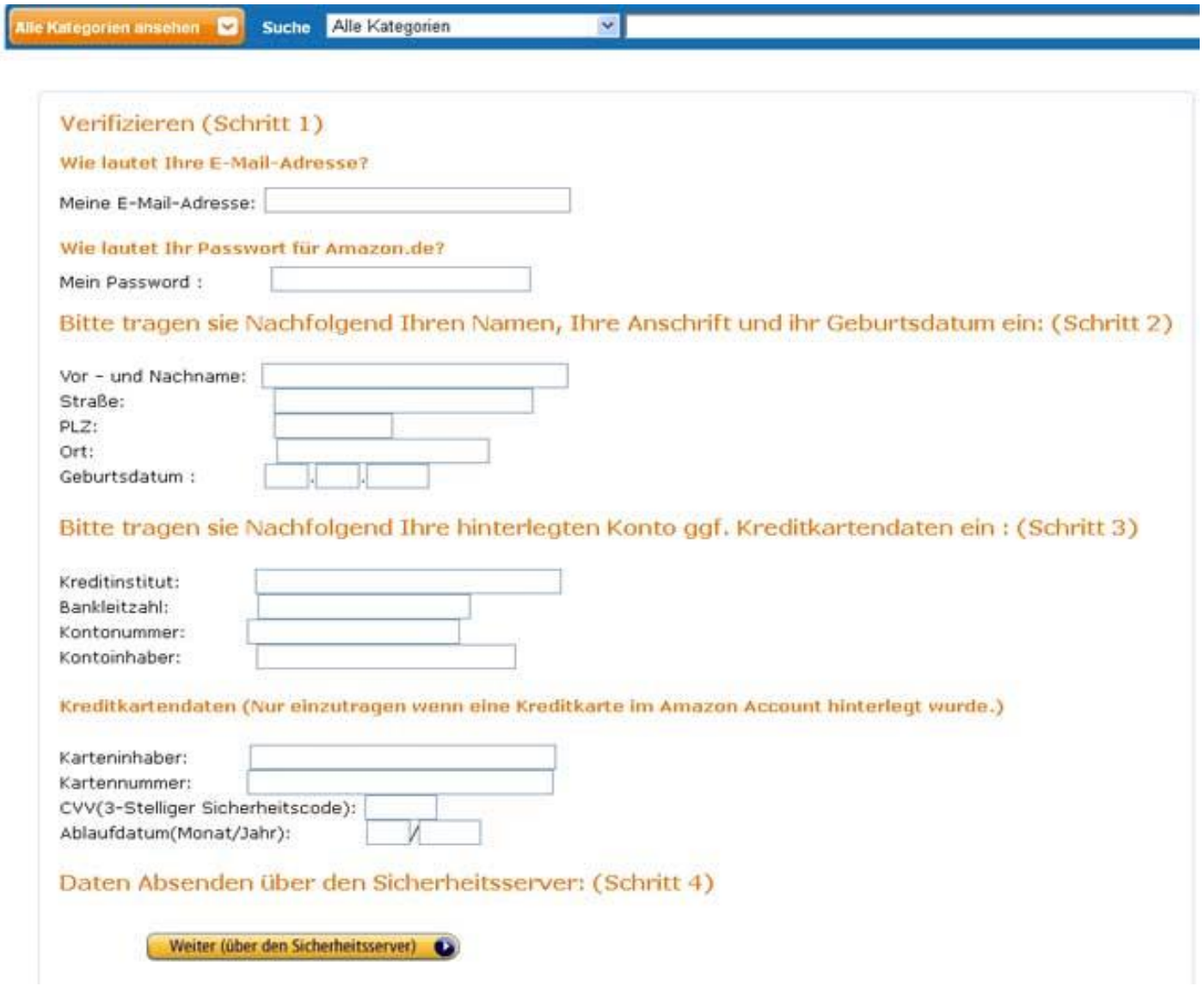
Konto jetzt verifizieren

Der Link zur Verifikation zeigt auf http://www.**amazon-kundencenter**.de/verifizierung.

Die Domain www.amazon-kundencenter.de hat jedoch mit www.amazon.de nichts zutun!

Klicken sie auf den Link, gelangen sie zur Webseite der Kriminellen, die der Webseite von Amazon „täuschend ähnlich sieht“…

Typische Phishing-Webseite mit Amazon-Layout



„Trojaner“

Was ist ein „Trojaner“?

- Software, die vorgibt nützlich zu sein oder die heimlich an nützliche Software angebaut wurde (Das „Trojanische Pferd“) und dann im Hintergrund arbeitet (Die Soldaten, die nachts aus dem Trojanischen Pferd kommen)

  => Vorsicht bei kostenlosen Angeboten

Umgangssprachlich wird unter dem **Begriff regelmäßig aber jede beliebige Schadsoftware** zusammengefasst.

„Trojaner“

Wie kommen Trojaner auf meine Geräte?

- Aktives öffnen einer Datei (E-Mail-Anhang , Download, USB-Stick, CD, andere Quellen)
- Durch Sicherheitslücken im eigenen Computer <= aktive Ausnutzung durch Angreifer

Was ist das Ziel eines Trojaners?

- Stehlen von Passwörtern
- Stehlen von Bankdaten oder Kreditkartendaten
- Selten Erpressung

Was kann ich tun?

- Virenscanner
- Installieren sie Softwareupdates unbedingt möglichst zeitnah
- Verschiedene Passwörter für verschiedene Anbieter

Spezialfall Onlinebanking-Trojaner

Was tun, wenn beim Onlinebanking eine merkwürdige Sicherheitsüberprüfung erfolgte oder eine Testüberweisung verlangt wurde?

- Internetverbindung trennen und Computer nicht mehr verwenden.
- Telefonische Mitteilung an die Hausbank, um evtl. bereits erfolgte Überweisungen zurückzurufen und/oder das Konto sperren zu lassen.
- Computer von Fachmann säubern lassen.
- Alle Benutzerkonten (E-Mail, Ebay, PayPal, pp.) von einem sicheren PC aus (!!!) auf Änderungen überprüfen und unbedingt alle Passwörter ändern.
- Alle Handlungen kurz dokumentieren (evtl. auch Fotos mit Handy/Kamera).
- Bei der nächstgelegenen Polizeidienststelle oder über die Onlinewache Anzeige erstatten.

Tipps zum Thema Onlinebanking

Was kann ich schon im Vorfeld tun?

- **Überweisungslimit niedrig wählen**
- **Verschlüsselung der Webseite prüfen („https://…“)**
- **Regelmäßig Kontostand/Umsätze prüfen**
- **Niemals öffentliche Computer für Geldgeschäfte verwenden**
- **Nutzen Sie die aktuellsten Verfahren für Online-Banking, die Ihre Bank bietet**
  - **chipTAN / smartTAN**

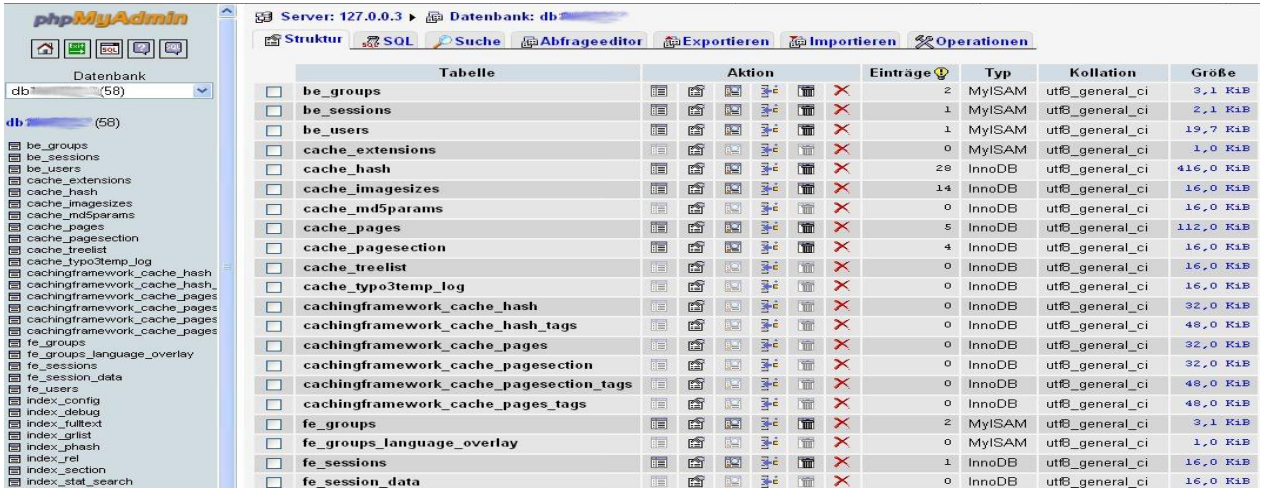
Hacking von Datenbanken:
Alles richtig gemacht – Daten trotzdem weg

Was sind Datenbanken überhaupt?

Die meisten von uns kaufen heutzutage im Internet ein. Die wenigstens machen sich aber Gedanken, was mit den Daten passiert, die man für die Bestellung angeben muss.

Die Bestelldaten bleiben in der Regel bei dem Anbieter gespeichert…praktisch für die nächste Bestellung, doch wo werden die Daten gespeichert?

Webseiten z.B. speichern in Datenbanken Artikel, Preise, Benutzerdaten, Bestellungen, …



Hacking von Datenbanken:
Alles richtig gemacht – Daten trotzdem weg

Und wie gelangen meine Daten nun an die Kriminellen?

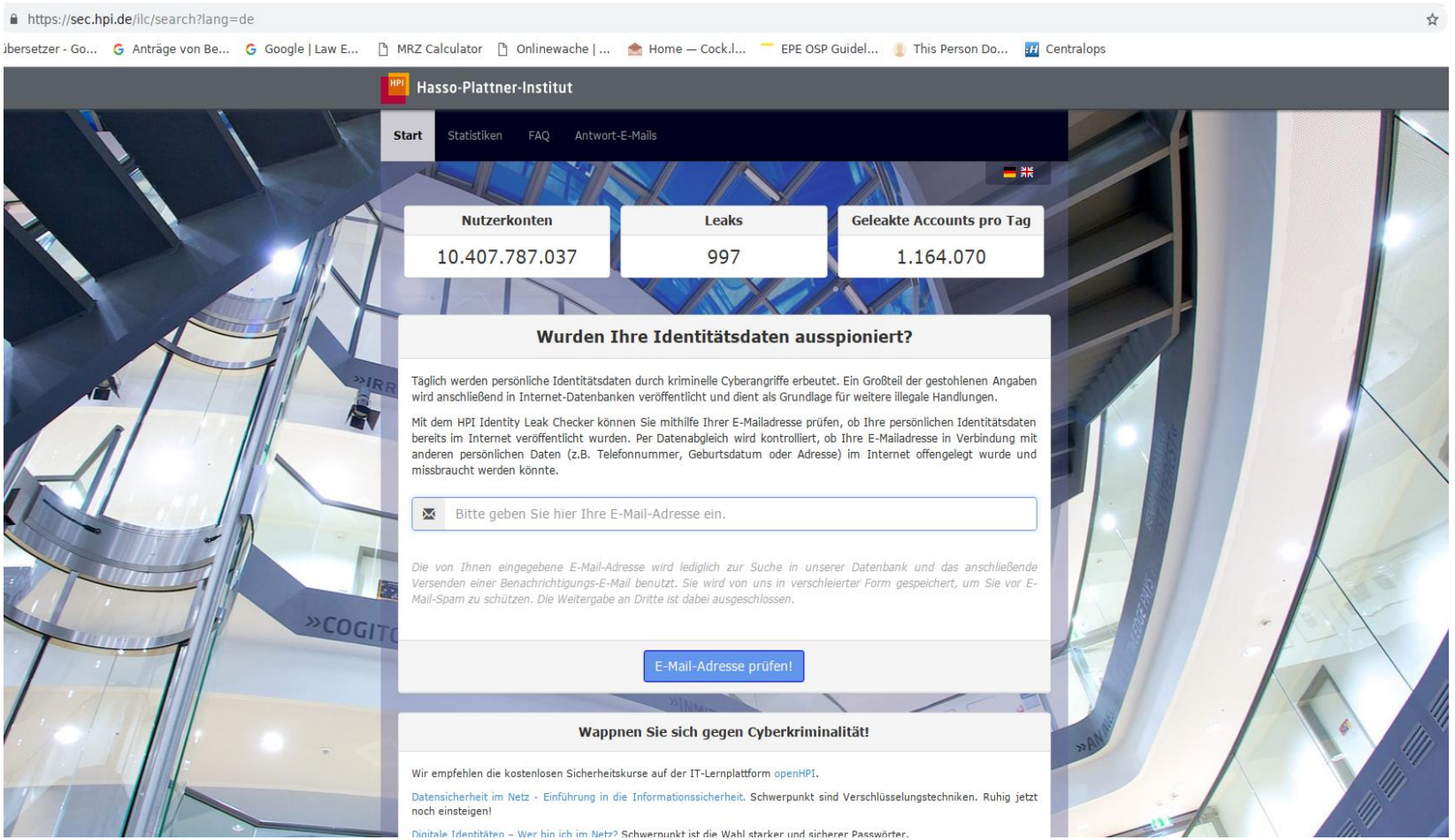
Durch Ausnutzung von **Sicherheitslücken** können die Täter an die Inhalte der Datenbanken gelangen und finden darin

- Namen
- Adressen
- Telefonnummern
- Kontodaten
- Kreditkarteninformationen
- E-Mail-Adressen
- manchmal Passwörter

Was kann ich tun?

Verschiedene Passwörter für verschiedene Anbieter verwenden

Hacking von Datenbanken:
Alles richtig gemacht – Daten trotzdem weg



SAARLAND

Was wir selbst preisgeben - Die Gefahren der sozialen Medien

Was versteht man eigentlich unter sozialen Medien?

„Soziale Medien“ sind digitale Medien, die es Nutzern ermöglichen, sich zu vernetzen und eigene Daten über das Internet zur Verfügung zu stellen (Facebook, Twitter, Blogs, YouTube, WhatsApp, etc.).

- Noch nie war es so einfach, der Welt persönliche Daten zur Verfügung zu stellen
- Noch nie war es so einfach, an Informationen anderer Menschen zu kommen
- Noch nie war es so einfach, fremde Menschen zu manipulieren oder zu erpressen
- Noch nie war es so schwer herauszufinden, wohin die eigenen Daten wirklich gehen
- Noch nie war es so schwer, Kontrolle über die eigenen Daten zu behalten/zurück zu erlangen

Geben Sie niemals Informationen im Internet preis, die Rückschlüsse auf ihre Passwörter geben! (Beispiel: Foto von eigenem Hund mit Namen „Blacky“ und Passwort „blacky01“)

Was wir selbst preisgeben -
Die Gefahren der sozialen Medien

Datenveränderung und Computersabotage

Von Sperrbildschirmen, Verschlüsselung und DDoS-Angriffen…

..und was all das mit Erpressung zu tun hat.

Die Anfänge der Ransomware – Ransomware 1.0

Was ist Ransomware?

Als Ransomware wird Schadsoft**ware** bezeichnet, die den Zugriff auf oder die Nutzung von Daten blockiert und zur Freigabe ein Lösegeld (engl. „**ransom**“) fordert.

Die erste Generation dieser Art von Software (Ransomware 1.0) blockiert **scheinbar** die Computernutzung bis Geld für die Freischaltung des Computers gezahlt wurde.

Merkmale

- Täter geben sich oft als Behörde aus
- Ihnen wird vorgetäuscht, der Computer sei wegen illegaler Handlungen gesperrt worden
- Es wird eine Lösung durch Bezahlung von Geld angeboten (Paysafe-, Amazon-, iTunes-Guthaben, ..)
- Oft Zeitdruck

Was kann ich tun?

- Niemals bezahlen!
- Updates!
- Computer von Fachmann freischalten lassen

Beispiele für klassische Ransomware 1.0

Beispiele für klassische Ransomware 1.0

Ransomware 2.0 oder wie Verschlüsselung zur Bedrohung wurde

Was hat sich geändert ?

- Im Hintergrund werden **alle wichtigen Daten** verschlüsselt
- Man braucht nun einen **Schlüssel**, um an die eigenen Daten zu kommen
- Der Schlüssel kostet Geld

MASSIVES PROBLEM FÜR UNTERNEHMEN !

Was kann ich tun?

- regelmäßige Backups (auch offline)
- Updates
- Vorsicht bei verdächtigen Mails
- Computer direkt ausschalten und an Fachmann geben
- Anzeige bei Polizei erstatten

Beispiel Ransomware 2.0

Ransom Note

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://6dtxgqam4crv6rr6.tor2web.org/ECCEADDE847A1F1A
2. http://6dtxgqam4crv6rr6.onion.to/ECCEADDE847A1F1A
3. http://6dtxgqam4crv6rr6.onion.cab/ECCEADDE847A1F1A

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 6dtxgqam4crv6rr6.onion/ECCEADDE847A1F1A
4. Follow the instructions on the site.

!!! Your personal identification ID: ECCEADDE847A1F1A !!!

Beispiel Ransomware 2.0

WARNUNG

Wir verschlüsseln Ihre Dateien mit Crypt0L0cker Virus

Ihre wichtigen Dateien (einschließlich der an den Netzwerk-Festplatten, USB, etc.): Fotos, Videos, Dokumente, etc. wurden mit Crypt0L0cker Virus verschlüsselt. Der einzige Weg, um Ihre Dateien wiederherzustellen, ist an uns zu zahlen. Andernfalls wird Ihre Dateien verloren gehen.

Vorsicht: Entfernen von Crypt0L0cker nicht wiederherstellen Zugriff auf Ihre verschlüsselten Dateien.

Zum Wiederherstellen von Dateien müssen Sie bezahlen.

Um die Dateien zu öffnen unsere Website http://x5sbb5qesp6kzwsh.questpul.pl/dvwmx7.php?user_code=3nmjaal&user_pass=2570 und folgen Sie den Anweisungen wiederherzustellen.

Wenn die Website nicht verfügbar ist, folgen Sie bitte diesen Schritten:
1. Herunterladen und TOR-Browser von diesem Link installieren: https://www.torproject.org/download/download-easy.html.en
2. Nach der Installation der Browser ausgeführt wird und die Adresse eingeben: http://xiodc6dmlzahhijj.onion/dvwmx7.php?user_code=3nmjaal&user_pass=2570
3. Folgen Sie den Anweisungen auf der Website.

SAARLAND

Beispiel Ransomware 2.0

Sprachaus wahl

Zeitdruck

SAARLAND

Beispiel Ransomware 2.0

SAARLAND

DDoS-Angriffe…
und wieso **Sie** Teil des Problems sein könnten

Was ist ein DDoS-Angriff?

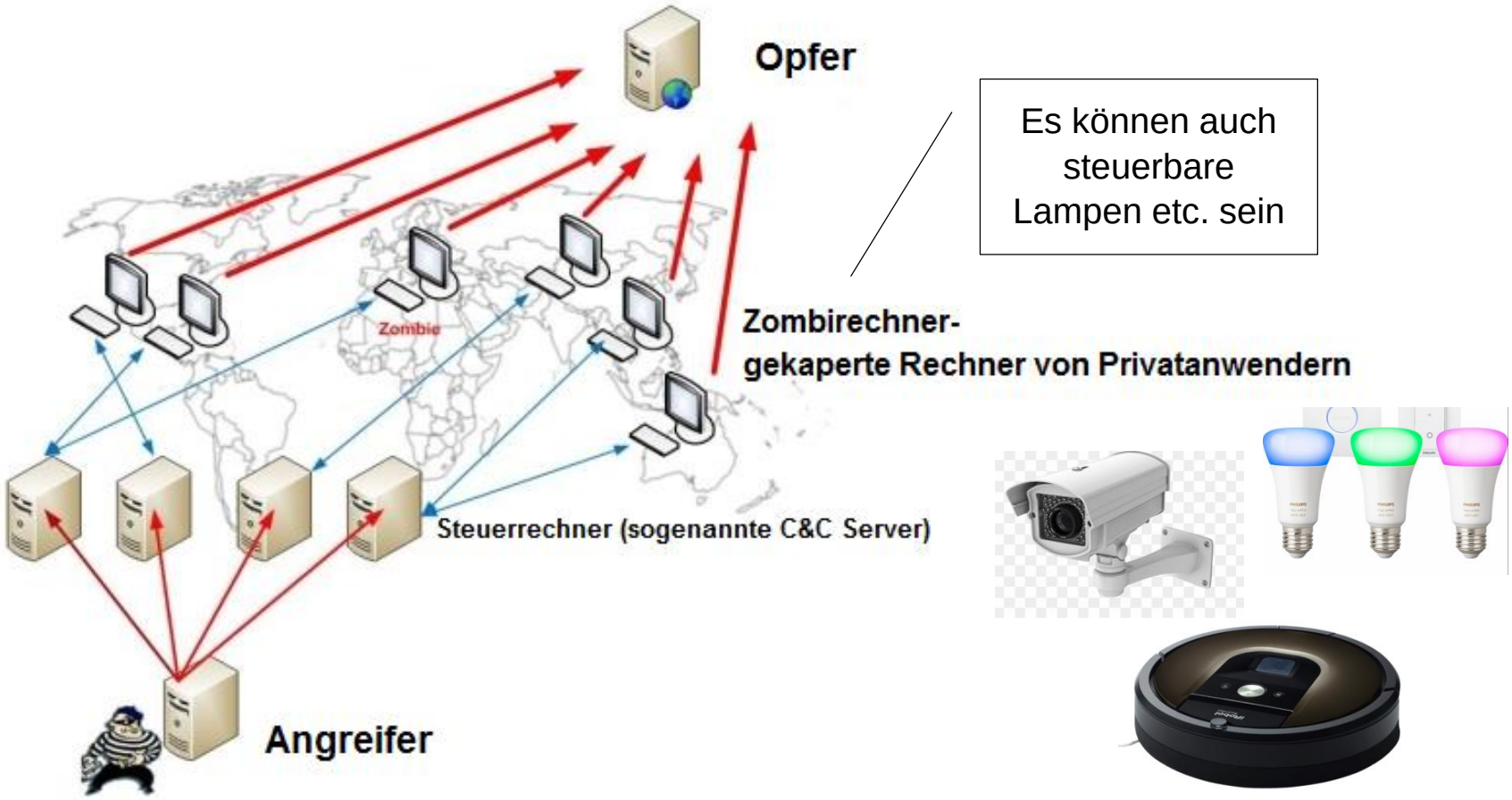
Ein DDoS-Angriff (Distributed Denial of Service) ist ein Angriff auf eine Webseite mit dem Ziel, diese für eine gewisse Zeit lahm zu legen.

Dazu schießen zehntausende oder hunderttausende Computer Datenpakete gleichzeitig auf das Ziel, welches dann solange den Dienst verweigert, bis der Ansturm aufhört.

Wo ist das Problem?

- Hoher Schaden für Unternehmen, die Geld mit ihrer Webseite verdienen
- Angreifer sind während des Angriffs oft nicht aufspürbar
- Angriffe kommen in der Regel von **privaten Computern** wie Ihrem

DDoS-Angriffe…
und wieso jeder von uns Teil des Problems ist



Es können auch steuerbare Lampen etc. sein

SAARLAND

DDoS-Angriffe…
und wieso jeder von uns Teil des Problems ist

Was kann ich tun?

- Updates
- Wenn der PC nicht gebraucht wird: herunterfahren.
- Keine Software aus unsicheren Quellen installieren
- Keine Datenträger, die man auf der Straße findet, verwenden
- Geräte, die nicht mit dem Internet verbunden sein müssen (z.B. Spülmaschine), nicht mit dem Internet verbinden

Betrug und Social Engineering – Wovor ich Sie noch warnen wollte…

- **Waren- und Warenkreditbetrug**
- **Waren- und Finanzagenten**
- **Love Scam und Social Engineering**

Warenbetrug – wenn bestellte Ware niemals eintrifft

Was ist Warenbetrug?

Sie bestellen oder kaufen Ware und erhalten sie nicht oder nicht so, wie erwartet.

Wie kann das passieren?

- Straftäter erstellen gerne selbst Onlineshops und verkaufen Ware, die sie gar nicht besitzen
- Der eBay-Account eines renommierten Händlers wird gehackt

Warenkreditbetrug – wenn jemand anderes für Sie bestellt

Was ist Warenkreditbetrug?

Ihnen wird Geld abgebucht für Ware, die Sie nicht bestellt und auch nicht bekommen haben.

Wie kann das passieren?

- Eine Datenbank mit Ihren Kreditkartendaten oder Passwörtern wurde gehackt
- Sie hatten ein zu einfaches Passwort für PayPal, das E-Mail Postfach oder ähnliche Anbieter
- Sie sind auf eine Phishing Kampagne hereingefallen
- Ihre Daten wurden ausgespäht (Trojaner)

Warenbetrug und Warenkreditbetrug

Worauf sollte ich beim Onlineshopping achten?

- Updates
- Seriosität des Anbieters prüfen (Alter des Shops, Impressum, **Zahlungsmethoden**)
- Niemals an öffentlichen Computern Geldgeschäfte machen – auch nicht shoppen!
- Misstrauisch werden, wenn etwas zu billig ist oder (Zeit-)Druck aufgebaut wird (z.B. Countdowns)
- Auf Vorkasse verzichten und lieber etwas mehr Geld ausgeben

Waren- und Finanzagenten

Was sind Waren- und Finanzagenten?

Das sind Menschen, die entweder gutgläubig im Nebenerwerb oder mit krimineller Energie Waren oder Geld aus einer Quelle annehmen und an ein anderes Ziel weiterleiten.

Rekrutierung:

Waren- und Finanzagenten werden in der Regel über Jobangebote rekrutiert.

Beispiele:

- Nebenjob als Warenkontrolleur
- Nebenjob in Heimarbeit, man muss nur einfache Finanztransaktionen tätigen

Strafbarkeit und Haftung:

Grundsätzlich besteht der Verdacht der leichtfertigen Geldwäsche (§ 261 StGB – Freiheitsstrafe bis zu 2 Jahren oder Geldstrafe). Der Finanzagent wird ggf. in Regress genommen.

Waren- & Finanzagenten –
So schnell werden sie versehentlich Finanzagent

1. Sie **verkaufen ein Auto** im Internet für 10.000€
2. Ein Interessent meldet sich (oft aus dem EU-Ausland)
3. Er will das Auto im Auftrag eines anderen kaufen und überweist Ihnen 10.000€.
4. Er tritt vom Kaufvertrag zurück und schildert eine herzzerreißende Geschichte
5. Sie sollen 9.700 Euro bitte zurücküberweisen – aber auf ein anderes Konto
6. Sie dürfen die 300 Euro Differenz behalten – „für Ihre Unannehmlichkeiten“
7. Einige Tage später fordert ein Ihnen unbekannter Dritter seine 10.000€ zurück

Was ist passiert?

Täter haben die Zugangsdaten zum Bankkonto des Eigentümers der 10.000€ erlangt und Sie als Zwischenstation missbraucht, um Spuren zu verwischen und die Ermittlungen in die Länge zu ziehen und zu erschweren

Waren- & Finanzagenten –
So schnell werden sie versehentlich Finanzagent

Wie kann ich mich schützen?

- Stets die Beziehung zwischen Identität des Käufers und verwendeter Bankverbindung (Kontoinhaber/ausländische Bank) hinterfragen
- Niemals Geld per Western Union oder Treuhanddienste zurücküberweisen
- **Rücküberweisung ausschließlich auf Konto, von dem das Geld ursprünglich angewiesen wurde!**

Love Scam
Liebe und Triebe…

Der typische Ablauf einer „Sexuellen“-Erpressung

1. Kontaktaufnahme in Single-Börsen oder Sozialen Netzwerken (z.B. Facebook)
2. Aggressives flirten
3. Umstieg von Text auf Videobild (z.B. Skype-Messenger, WhatsApp)
4. Der Täter / die Täterin entkleidet sich und fordert dazu auf, dies auch zu tun
5. Ohne Ihr Wissen wird das Video aufgezeichnet
6. Nach Fertigstellung des Videos werden Sie damit erpresst, denn durch den Facebook-Kontakt kennen die Täter Ihre Kontakte und drohen damit, Sie öffentlich bloß zu stellen

SAARLAND

Love Scam
Liebe und Triebe…

Trittbrettfahrer: „Sextorsion“

Oft will eine E-Mail **vortäuschen**, dass der Computer gehackt worden sei und es zuvor bereits **heimliche Aufnahmen** gegeben habe. Man droht mit der Veröffentlichung, sofern kein Geld bezahlt wird.

Diese Aufnahmen gibt es dann nicht. Es ist nichts passiert!

Hier werden massenhaft E-Mails automatisiert an verschiedene Empfänger verschickt. Es findet hier **KEIN** Ausspähen von Daten/ Aufnehmen von Videos statt, es gibt nur diese eine Spam-E-Mail. Durch Anzeige der **eigenen E-Mailadresse** als Absenderadresse wird Authentizität vorgetäuscht.

Love Scam
Liebe und Triebe…

Romance-/Love Scam

1. Kontakt über **Single-Börse** oder teilweise auch z.B. Kleinanzeigen
2. Sie werden mit irgendeiner Geschichte konfrontiert (oft Notlage, aber auch Romantik, Zuneigung, Flirten)
3. Sie werden durch die drei klassischen Antriebe **Liebe, Mitleid oder Gier** manipuliert
4. Sie transferieren Geld ins Ausland
5. Solange Sie noch Geld haben und weiterhin überweisen, wiederholt sich der Kreislauf ab Punkt 2 immer weiter (oft Jahre, bis zum Bankrott)
6. Ihr transferiertes Geld ist ohne Gegenleistung weg.

Wenn Microsoft am Telefon ist…

Supportanrufe aus indischen Callcentern

- Anruf von vermeintlichem Microsoftmitarbeiter (meist englischsprachig) oder Sperrbildschirm mit Hinweis auf eine Supporthotline
- Mitteilung über angebliche Schadsoftware auf Computer
- Telefonische Anleitung zur Installation von Fernwartungssoftware
- Reparatur via Fernzugriff und Verkauf von Sicherheitszertifikaten für Windows für 80 € – 200 € -> per Kreditkarte wird bezahlt…
- Veränderungen an Ihrem Computer über Fernwartungssoftware durch Täter, die z.B. das Ausspähen von Bank- und Kreditkartendaten und Passwörtern erlauben.

Tipps für Chats, Foren, Soziale Netzwerke und Handelsplattformen

Wie sollte ich mich grundsätzlich verhalten?

- Seien Sie zurückhaltend mit persönlichen Informationen. Es gibt kein Zurück!
- Überprüfen Sie so viele Informationen wie möglich
- Lassen Sie sich nicht auf andere, externe Seiten locken
- **Lassen Sie sich nicht unter Druck setzen!**
- Überweisen Sie kein Geld und schicken sie keine Waren an „neue Bekannte/Freunde/ Liebschaften“
- Wenden Sie sich an die Polizei, wenn Sie fürchten an einen Betrüger geraten zu sein
- Mit Google recherchieren

SAARLAND

Aktuelles Phänomen – Spam SMS

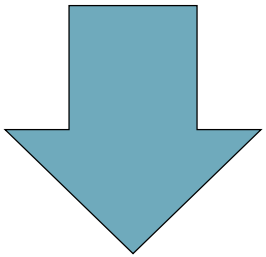
SAARLAND

Wie kann ich mich schützen?

Allgemeine Tipps zum Thema Sicherheit für den Alltag

Wie kann ich mich schützen?

Absolute Sicherheit ist nicht zu haben!



Unser Ziel muss es sein, mit einfachen Mitteln ein möglichst hohes Maß an Sicherheit zu erreichen!

Wie kann ich mich schützen?

Generelle Handlungsempfehlungen

- **Updates** für Betriebssystem & sonstige Software möglichst zeitnah durchführen
- **Antiviren-Software** installieren und aktiv und aktuell halten
- Lösungen wie „**Browser in the Box**“ verwenden
- Für verschiedene Dienste (E-Mail, Ebay, PayPal, Amazon, Foren) **verschiedene Passwörter** benutzen
- E-Mails, auch von vermeintlich bekannten Absendern, **grundsätzlich misstrauen**. Niemals unbekannte **Datei-Anhänge** oder Rechnungen öffnen
- Vermeiden sie das Klicken von **Links in E-Mails**. Gehen sie lieber selbst über die Eingabe der Webadresse im Browser auf Webseiten (Amazon, PayPal …)
- Niemals Passwörter, Zugangsdaten, wichtige Personendaten oder Personalausweisscans ungeschützt auf dem Computer speichern (Passwort-Safe, Zettel nutzen)

Vielen Dank für Ihr Interesse!

Fragen? Wünsche? Anregungen?

Maurice Marrali

Landespolizeipräsidium des Saarlandes
Dezernat LPP 222 Cybercrime
Hellwigstraße 8-10
66121 Saarbrücken
0681-962-2432