IT-Sicherheit:
Aktuelle Bedrohungen + rechtliche Rahmenbedingungen

DI Martin Schober

IT-& Cybersecurity
Cloud Consultant
Sprecher IT-Security Experts Group Salzburg

Breaking News

ALERT:

AVAST

CCleaner 2,2 Mio Installationen infiziert

Bitte überprüfen Sie die Installation!

DI Martin Schober

- Gründer: MSc-martinschober.com 2003
  - Mitarbeit: Siemens UMTS-Standard
  - Baxter BioScience: TQM-Mangement
- IT- & Cybersecurity
- Cloud-Consultant für Outsourcing, SLAs
- Sprecher der IT-Security Experts Group Salzburg
- ISO & BSI Auditor (IT-Sicherheit, ISO27001, BSI GS)
- Data & IT-Security Expert zert. lt. ISO 17024
- **Arbeite gerade an einem IT-ThinkTank**

Agenda

- Einführung
- Aktuelle Bedrohungen & „selbstgemachte“ Probleme
- EU Datenschutzgrundverordnung (DSGVO)
- Fazit
- Diskussion

Diebstahl, Raub und Betrug

- Strafbare Handlungen
- „Verbrecher, Gangster, Strizzis“
- Mut, gefährlich, wird leicht gefasst

Was hat das mit dem Internet zu tun?

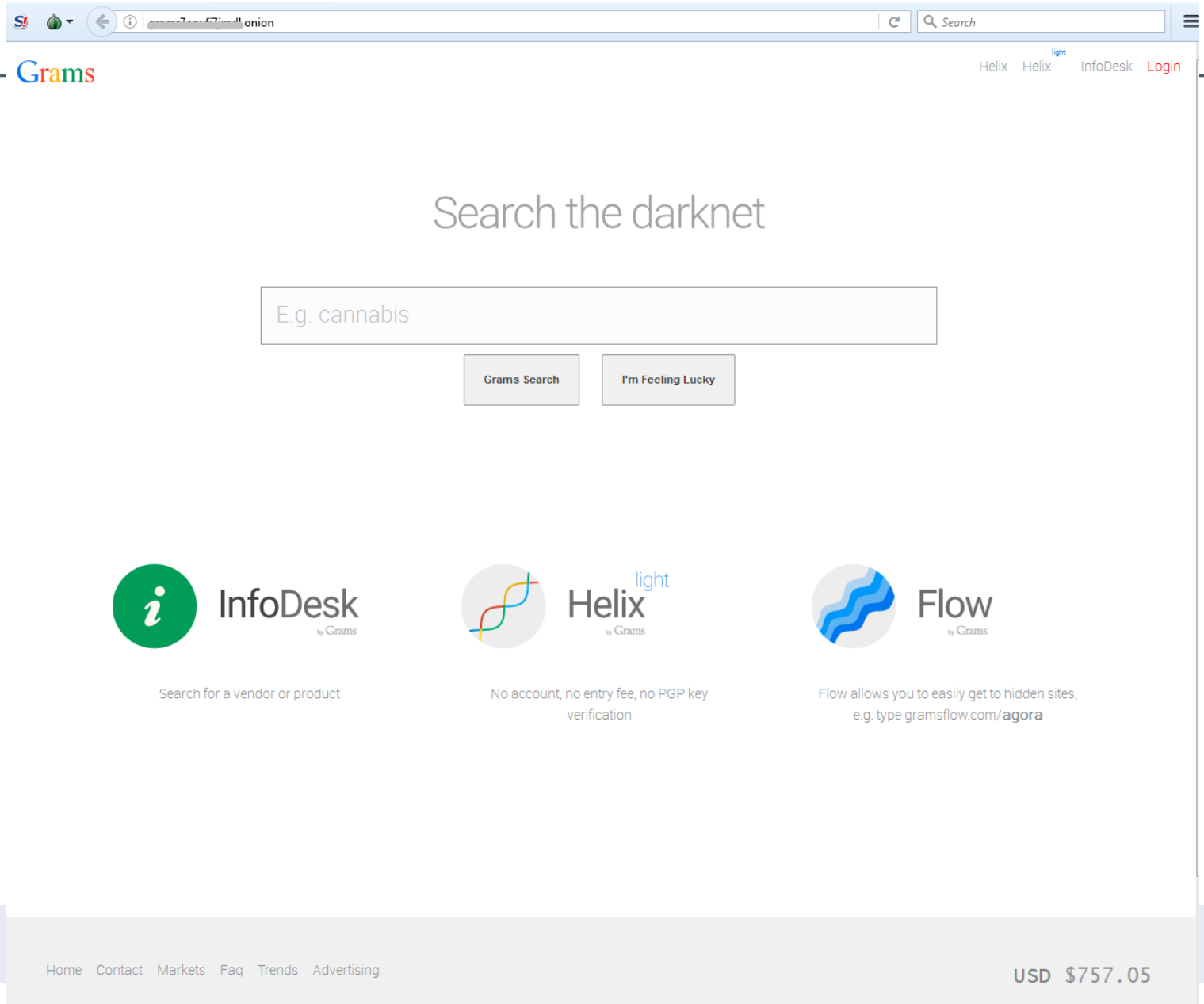
- **Computer Crime!**
- **Einfacher, sauberer**
- **Hacken ist „cool“**


DATA SECURITY
HACKER
PASSWORD
IDENTITY THEFT
© Alamy

Strafrechtliche Verantwortlichkeiten Computer Crime

§	WAS	WIEVIEL
51 DSG	Datenverwendung in Gewinn- oder Schädigungsabsicht	bis 1 Jahr
118a StGB	Widerrechtlicher Zugriff auf ein Computersystem	bis 3 Jahre
119 StGB	Verletzung des Telekommunikationsgeheimnisses	bis 6 Monate
119a StGB	Missbräuchliches Abfangen von Daten	bis 6 Monate
120 StGB	(Missbrauch von Tonaufnahme- oder Abhörgeräten) Abs. 2a Aufzeichnung von Nachrichten	(bis 1 Jahr) bis 3 Monate
126a StGB	Datenbeschädigung	bis 5 Jahre
126b StGB	Störung der Funktionsfähigkeit eines Computersystems	bis 5 Jahre
126c StGB	Missbrauch von Computerprogrammen oder Zugangsdaten	bis 6 Monate
148a StGB	Betrügerischer Datenverarbeitungsmissbrauch („Computerbetrug“)	bis 10 Jahre
225a StGB	Datenfälschung	bis 1 Jahr

Das „böse“ Darknet



/results

Search

Grams

meth

How to InfoDesk Helix Login

About 2590 results for 'meth' (0.4987 seconds)

Advanced Search

Top Notch Meth 1 Gram

pwoah7foa6au2pul.onion/listing.php?id=189981 **Alphabay**

We are new to the darknet but not new to the dope game This is top shelf meth straight from the border It burns clean and has legs behind it Once you try this you ll be back Orders will be shipped in a USPS priority envelope

Vendor powderhouse **Price** ฿0.04937505 **Location** United States

0 5 gram rasmic dl **meth**

pwoah7foa6au2pul.onion/listing.php?id=18818 **Alphabay**

This **meth** is derived from P2P Several acid base extractions fractional vacuum distillation crystallization with hcl vacuum filtration washing and drying makes this **meth** extremely pure and is technically more purer then its ephedrine based cousin But this is racemic methamphetamines it contains both entaniomers This means that it is a 50 mixture of right handed and left handed molecules dl **meth** This...

Vendor misterhotice **Price** ฿0.02228118 **Location** Belgium

(0)

0,04 XBT :~ 60,- EUR

1 gram rasmic dl **meth**

pwoah7foa6au2pul.onion/listing.php?id=18814 **Alphabay**

This **meth** is derived from P2P Several acid base extractions fractional vacuum distillation crystallization with hcl vacuum filtration washing and drying makes this **meth** extremely pure and is technically more purer then its ephedrine based cousin But this is racemic methamphetamines it contains both entaniomers This means that it is a 50 mixture of right handed and left handed molecules dl **meth** This...

Vendor misterhotice **Price** ฿0.04458876 **Location** Belgium

(0)

5 gram rasmic dl **meth**

pwoah7foa6au2pul.onion/listing.php?id=18817 **Alphabay**

This **meth** is derived from P2P Several acid base extractions fractional vacuum distillation crystallization with hcl vacuum filtration washing and drying makes this **meth** extremely pure and is technically more purer then its ephedrine based cousin But this is racemic methamphetamines it contains both entaniomers This means that it is a 50 mixture of right handed and left handed molecules dl **meth** This...

Set currency

BTC USD EUR GBP AUD

Market Chart

Market Status

Market Alerts

No Warnings

Also by Grams

Helix

Helix light

Flow

InfoDesk

DDoS kaufen?

VDOS

How do I purchase a vDos plan?

Purchasing a booter plan is easy and only takes a few minutes, we accept the following payment methods, based on your billing country/region and the currency in which you want to pay to make it an easy, secure and a quick shopping experience for you.

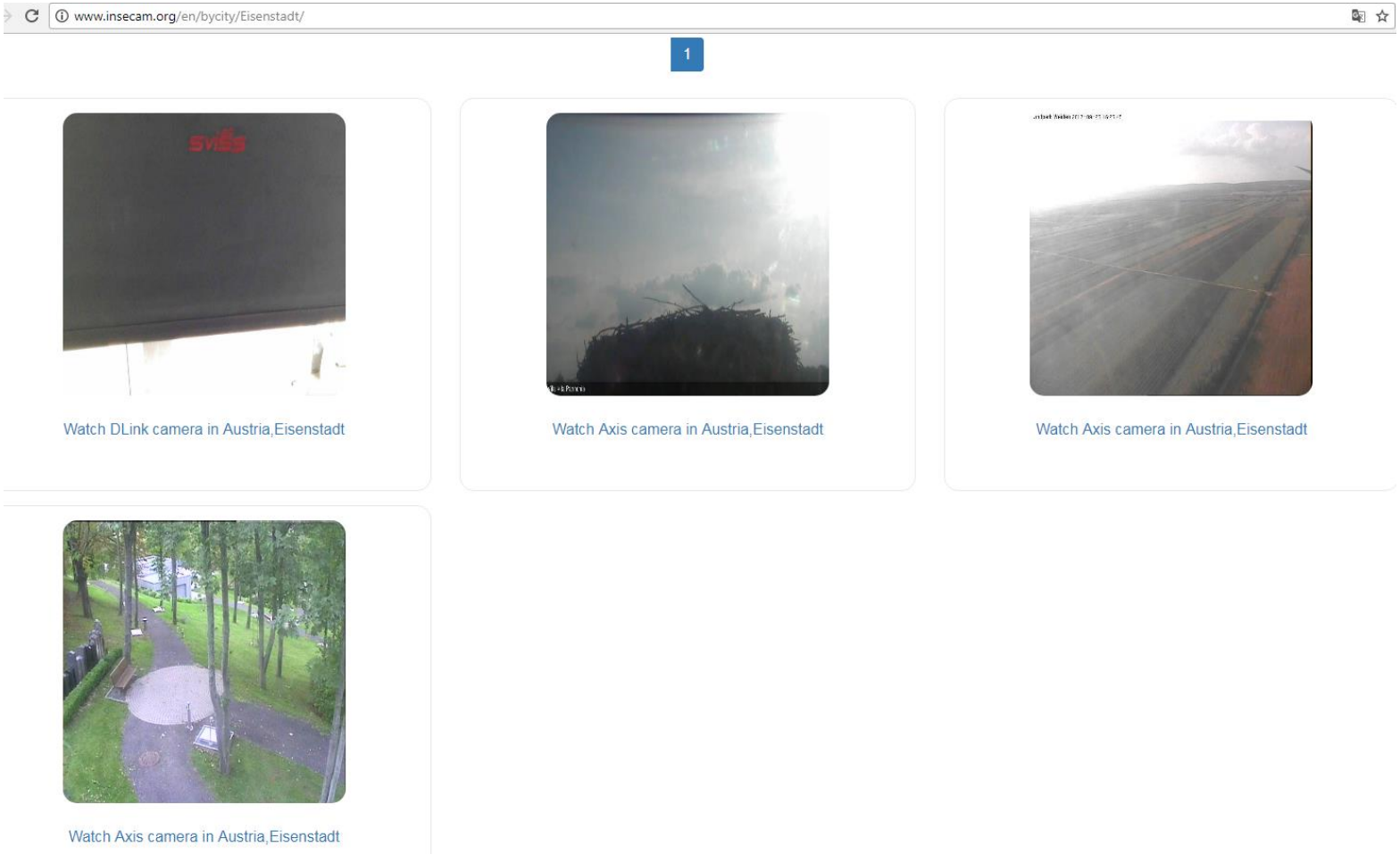
Bitcoin, we believe in the huge potential of this new digital currency.

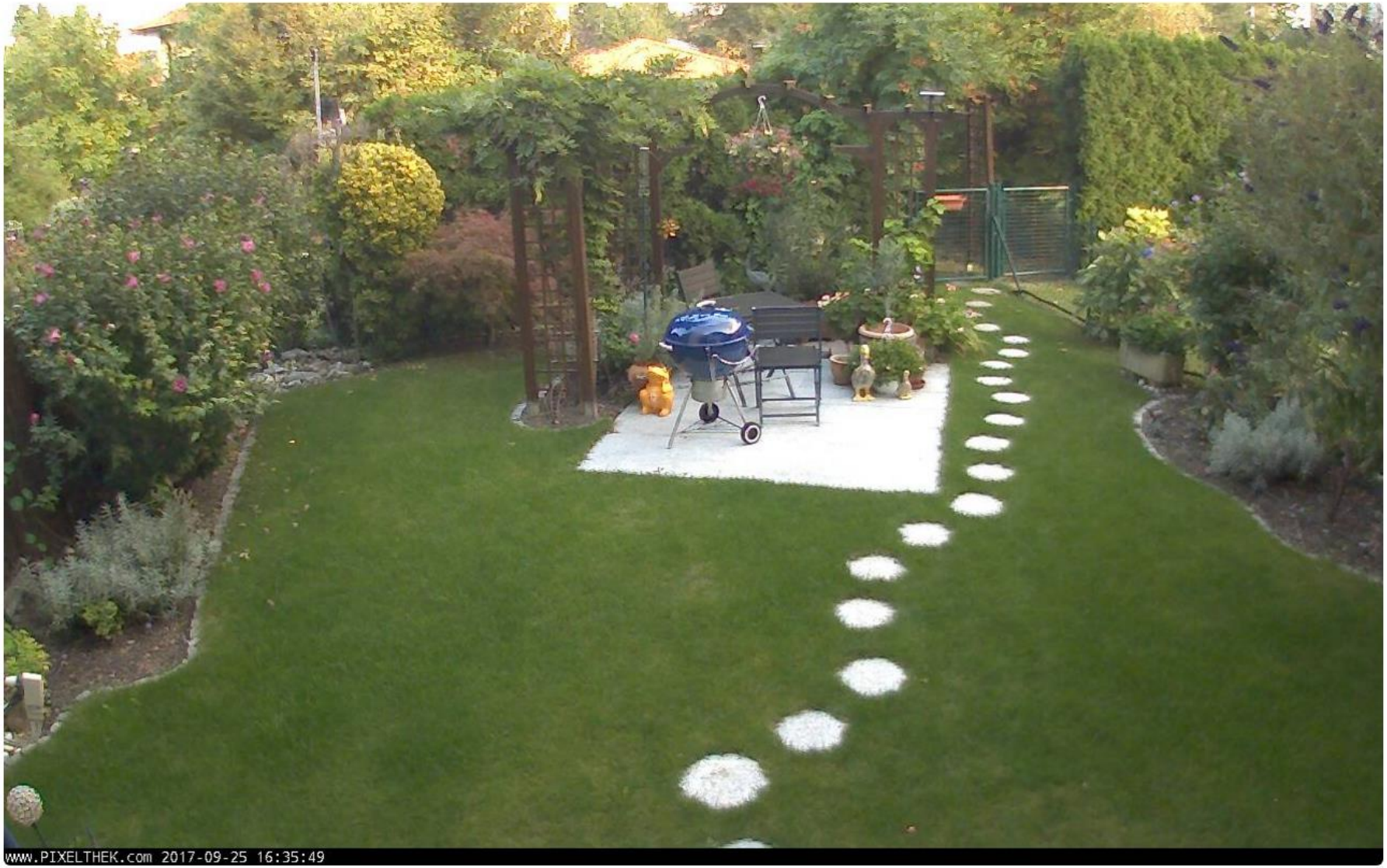
Pricing Lists

Select the best package based on your usage needs and size of business.

Bronze	Silver	Gold	VIP
$19.99 /monthly	$29.99 /monthly	$39.99 /monthly	$199.99 /monthly

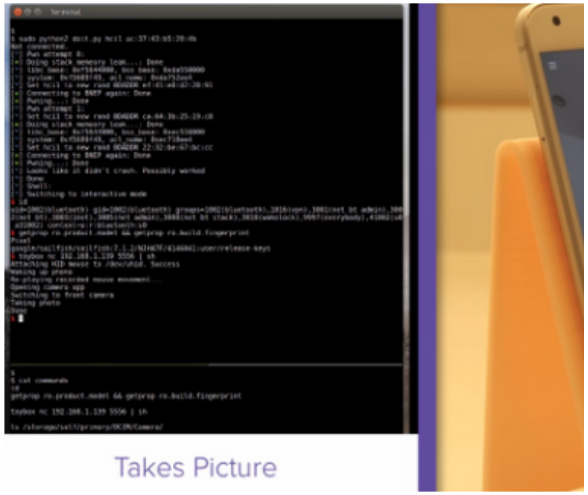
Bedrohungen selbst gemacht ->insecam.org




www.PIXELTHEK.com 2017-09-25 16:35:49

BlueBorne: Android, Linux und Windows angreifbar

13.09.2017 14:30 Uhr – Fabian A. Scherschel



Unbemerkter Angriff auf ein Android-Handy (Bild: Armis)

Millionen, vielleicht sogar Milliarden, von Geräten mit Bl unbemerkt über das Funkprotokoll angegriffen werden. können auf diese Weise gar komplett übernommen werd

Eine Reihe von Sicherheitslücken in den Umsetzungen de Android, Linux und Windows können von Angreifern missl beliebigen Schadcode auf dem Zielgerät zur Ausführung z Lücken im Zuge der Juli- und September-Patchdays gesch ebenfalls bereits Patches. Linux auf dem Desktop ist am a und zu allem Überfluss stehen hier Sicherheitsupdates bis war nur bis Version 10.0 angreifbar.

Angriff aus bis zu zehn Metern Entfernung

Entdeckt wurden die Lücken von der Sicherheitsfirma Arn im Internet of Things (IoT) spezialisiert ist und die Schwac BlueBorne getauft hat. Um einen Angriff zu starten, muss zehn Meter Entfernung zum Zielgerät befinden und das Op aktiviert haben. Der Angriff nutzt aus, dass Bluetooth-Ger Kommunikationspartnern suchen. Er soll auch funktionie bereits eine Verbindung zu einem anderen Gerät aufgebau Zuge der Attacke nicht, dass es angegriffen wird, während ausführt. Der ganze Angriff dauert nicht länger als zehn Se

Samsung stopft Blueborne-Lücke auf einigen Galaxy-Smartphones

25. September 2017 Kategorie: Android, Backup & Security, geschrieben von: Sascha Ostermaier

BlueBorne

Die Blueborne-Lücke sorgte kürzlich für Aufsehen, zahlreiche Geräte sind über eine Lücke in der Bluetooth-Schnittstelle angreifbar. Sind die Geräte mit dem Internet verbunden, kann nach einem Angriff Malware nachgeladen werden, alles Dinge, die man nicht möchte. Mit etwas Glück bekommt man für sein betroffenes Gerät (auch IoT-Geröte sind betroffen) ein Update, mit Pech bleibt man dauerhaft angreifbar, wenn man eben kein Update bekommt. Auf dieses warten auch viele Smartphone-Nutzer, gute Nachrichten gibt es an dieser Stelle von Samsung.

Während Android-Nutzer mit Security-Patch-Level September bereits auf der sicheren Seite sind, ist der Patch für die wenigsten überhaupt schon verfügbar. Aber Samsung hat die Blueborne-Lücke bereits mit den letzten aktuellen Updates gefixt, auch wenn diese nicht mit dem September-Patch versehen waren. Geräte wie das Galaxy S7, Galaxy S5, Galaxy Note 8 oder auch das Galaxy A5 erhielten bereits ein entsprechendes Updates mit Blueborne-Fix auch ohne September-Patch.

Unterdessen sind die Updates für Galaxy S8 und S8+ noch nicht unterwegs, das könnte sich aber schnell ändern. Ob es dann überhaupt noch einen September-Patch geben wird oder das dann gleich mit in den Oktober-Patch integriert wird, bleibt indes abzuwarten. Um zu überprüfen, ob Euer Android-Smartphone noch von der Blueborne-Lücke betroffen ist, könnt Ihr diese App verwenden.

Ein neuer Erpressungstrojaner fordert Nacktbilder statt Bitcoin von seinen Opfern

LORENZO FRANCESCHI-BICCHIERAI
Sept. 22 2017, 3:04pm

Screenshot: Twitter

Untermalt mit beschwingter Hintergrundmusik und mit grinsenden Lokomotiven stellt diese Ransomware eine dreiste Forderung.

VERBOTENE SENDEANLAGE

Spionage im Kinderzimmer: Puppe Cayla wird verboten

von Barbara Wimmer 17.0

Die smarte Puppe Cayla wird in De
strafbar zu machen. - Foto: VKI

VERBOTENE SENDEANLAGE

Spionage im Kinderzimmer: Puppe Cayla wird verboten

Die E
sma
verb
Cayl

SI
BARB

Rechtsgutachten

„Es sprechen entscheidende Gründe dafür, dass die Puppe eine verbotene Sendeanlage im Sinne des § 90 Telekommunikationsgesetz ist. Jedes bluetoothfähige Gerät in Reichweite von etwa zehn Metern kann eine Verbindung zu ihr aufbauen und Lautsprecher und Mikrofon nutzen. In einem Versuch hatte ich auch über mehrere Wände hindurch auf die Puppe Zugriff. Es fehlt an eingebauten Sicherungen", sagt Hessel.

In Folge kam auch die deutsche Bundesnetzagentur zu demselben Schluss. Der Verkauf von Calya wird daher in Deutschland verboten. Doch das ist nicht alles: Auf den Besitz von „verbotenen Sendeanlagen" stehen Strafen von bis zu zwei Jahren Haft. Betroffene Eltern, die das Spielzeug für ihr Kind gekauft haben, müssen die Puppe also vernichten. Dazu rät zumindest die Bundesnetzagentur.

Kritik von Konsumentenschützern

Auch in Österreich hat der Verein für Konsumenteninformation vor kurzem vor dem smarten Spielzeug gewarnt. Die Puppe sei ein Datenschutzrisiko und eine „Spionin im Kinderzimmer". Mit einem bluetoothfähigen Smartphone könne „jeder ganz leicht durch die eingeschaltete Puppe sprechen und auch alles in ihrem Umfeld mithören", weil die Verbindung völlig ungesichert sei. „Dieses Sicherheitsrisiko muss dem Unternehmen schon länger bekannt sein. Geändert hat sich aber wenig", kritisiert Ulrike Docekal vom VKI.

Allerdings ist ein Verbot, wie es in Deutschland erfolgt ist, hierzulande nicht möglich. „Wir haben eine andere Rechtslage, die

Der “Hum

- *“Practi*
  mather
  to brea
  broken
- Streuat
  - Bot
- Gezielt
  - Soc
  - Adv
  - Wat
  - Spe

The Dirty Hackers Who Steal Passwords for Jealous Lovers

JOSEPH COX
Jun 7 2017, 6:30pm

Phishing really is a threat when the hackers are closer to home.

SHARE TWEET

This story is part of When Spies Come Home , a Motherboard series about powerful surveillance software and other techniques ordinary people use to

Internet of Things Insecurity – Botnet Mirai

- Brian Krebs – Security Researcher
- 620Gbps(1 Tbps)
- Angriffsvektoren
  - Digitale Videorecorder
  - Consumer WLAN-Router
  - IP-Kameras
- GRE-basierter Angriff
- ~50.000 Devices

→ Gartner: 6.4 Milliarden Devices in 2016,
20.8 Milliarden in 2020 – 5.5 Million/Tag

Gegen wen kämpfen wir?

	Ungerichtet	Gerichtet	Staatlich motiviert
Extern	Viren, Trojaner, Schadsoftware, Bot-Netze, „Script Kiddies“	Anonymous, Betriebsspionage, Sabotage, Betrug, Social Engineering, DoS, CaaS	NSA Affäre, China, Russland, Israel,… (über 30 Nationen mit cyber warfare doctrine - 12 mit formellen Einheiten)
Intern	Unwissende MA, Fahrlässige MA, Verlust, „Drive-By“, Schadsoftware	„Vergraulte“ MA, Unberechtigte Nutzung, Diebstahl, Betriebsspionage, Sabotage	Standort- & branchenabhängig

Quelle: Stefan Jakoubi, SBA

Gegen wen kämpfen wir?

	Ungerichtet	Gerichtet	Staatlich motiviert
Extern	Viren, Trojaner, Schadsoftware, Bot-Netze, „Script Kiddies“	Anonymous, Betriebsspionage, Sabotage, Betrug, Social Engineering, DoS, CaaS	NSA Affäre, China, Russland, Israel,… (über 30 Nationen mit cyber warfare doctrine - 12 mit formellen Einheiten)
Intern	Unwissende MA, Fahrlässige MA, Verlust, „Drive-By“, Schadsoftware	„Vergraulte“ MA, Unberechtigte Nutzung, Diebstahl, Betriebsspionage, Sabotage	Standort- & branchenabhängig

Quelle: Stefan Jakoubi, SBA

Lösungsmöglichkeiten…

- Virenschutz?
  - ist „tot“
  - NUR noch als Zusatz
- Firewall?
  - Mit Intelligenz – zb. Thread Detection, KI
- Patches
  - Immer aktuell halten
- NAC, Clustering, VLANs, Segmentierung
  - Aufwändig
- SIEM / SDN uvm.
- Policies, Schulungen usw.

DSGVO – **D**aten**S**chutz**G**rund**V**er**O**rdnung

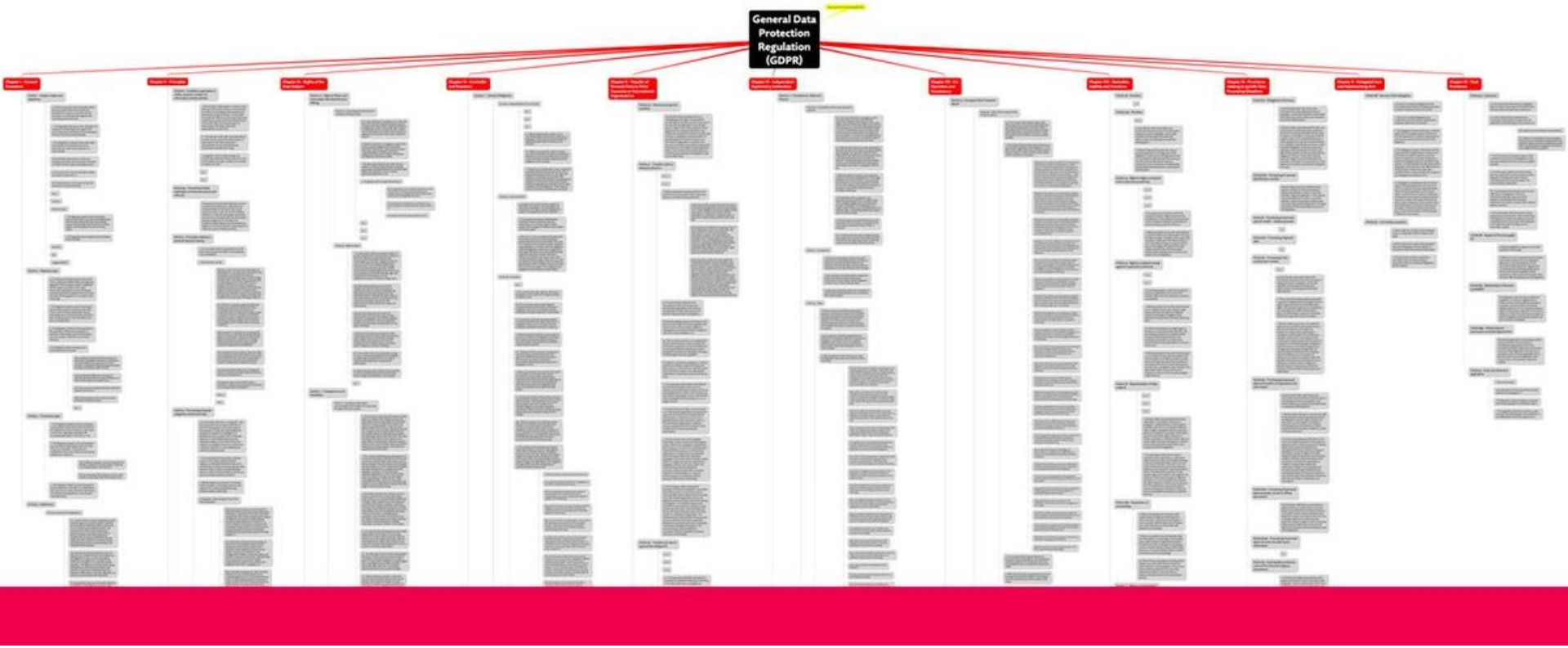
- *260 Seiten*
- *173 ErwGründe*
- *11 Kapitel*

- *99 Artikel*
- *Ende der Umsetzungsfrist:*

  25. Mai 2018

Dann ist DSG 2000 nicht mehr anwendbar & DSRL 96/46/EG *aufgehoben!*

DSGVO – **D**aten**S**chutz**G**rund**V**er**O**rdnung



Wichtigsten Änderungen in aller Kürze

- Einwilligung & Auskunftsrecht
- Umfassende Informationspflichten
- Entfall der DVR (Meldepflicht)
- Datenportabilität
- Recht auf Vergessenwerden
- Data Protection by Design/Default
- Dokumentationspflichten
- Datenschutz-Folgenabschätzung
- Meldung bei Vorfällen
- Hohe Strafen: 2% (10 Mio) und 4% (20 Mio) vom Jahresumsatz

Was tun als Unternehmer?

- Zeit bis Mai 2018:
  - Man muß **JETZT** anfangen
  - Projekt-Fahrplan erstellen - Timeline
  - Umsetzen und Dokumentieren
  - Risikomanagement – Kategorien definieren
  - Sicherheitskonzepte erstellen
  - Archivierung & Löschung definieren
  - GAP-Analyse: **Soll - Ist** Vergleich <- damit beginnen!

→ KMU Digital Förderung!

- ***https://www.kmudigital.at/***
- ***Bis zu € 1.000,- geförderte Beratungsleistung***

Angreifer vs. Verteidiger

Christiano Ronaldo

Bester Spieler 2016
Gehalt 2016: ca. **230 Millionen**

Manuel Neuer

Bester Torwart 2016
Gehalt 2016: ca. **15 Millionen**

Herausforderung >>Widerstandsfähigkeit<<

- Robustness / Robustheit
  - System hält Angriffen stand
  - Nicht definiert: was passiert wenn doch ein Angriff erfolgreich ist?

- Resilience / Widerstandsfähigkeit
  - System erfüllt auch unter Angriff / nach erfolgreichen Angriffen seine Hauptaufgaben
  - “Graceful Degradation“
  - “Anti-Fragility”

Die Vorteile auf unserer Seite sind ☺

Grundlegende Maßnahmen bezwingen einen Großteil aller Angriffe

Der Verteidiger hat Zeit, um Schwachstellen aufzudecken und sich vorzubereiten

Oft reicht es, etwas besser als die anderen zu sein

Man kann sich als Verteidiger unattraktiv machen, indem die Kosten für Angriffe erhöht werden

Wir schreiben das Jahr 2017!

Über 85% aller Cyber-Angriffe lassen sich durch grundlegende Maßnahmen und entsprechendes Sicherheitsbewusstsein verhindern

Ende

- Fragen
- Anmerkungen
- Diskussion

DI Martin Schober
IT- & Cybersecurity
IT-Security Expert
office@martinschober.com
+43.660.1517017