Dokumentation Weiterbildung IT-Systeme

Datenschutz und IT-Sicherheit „Fluch & Segen“

Wie Staaten, Nachrichtendienste und private Exploitanbieter den Datenschutz und die IT-Sicherheit aushebeln und dabei die Tür für Cyberkriminalität weit öffnen.

Dokumentation
Weiterbildung
IT-Systeme

Datenschutzbeauftragter

Heiko Langenhan
Geschäftsführer
Leiter IT- Systeme – externer Datenschutzbeauftragter

Mehr als 5 Jahre Erfahrung im Datenschutz
Consultant für IT-Infrastruktur-Lösungen

IT-Systeme
IT-Infrastruktur-Lösungen
Dienstleistung IT-Infrastruktur – Administration / Service & Support
externer Datenschutzbeauftragter
Analyse & Consulting IT-Security (VdS 3473)

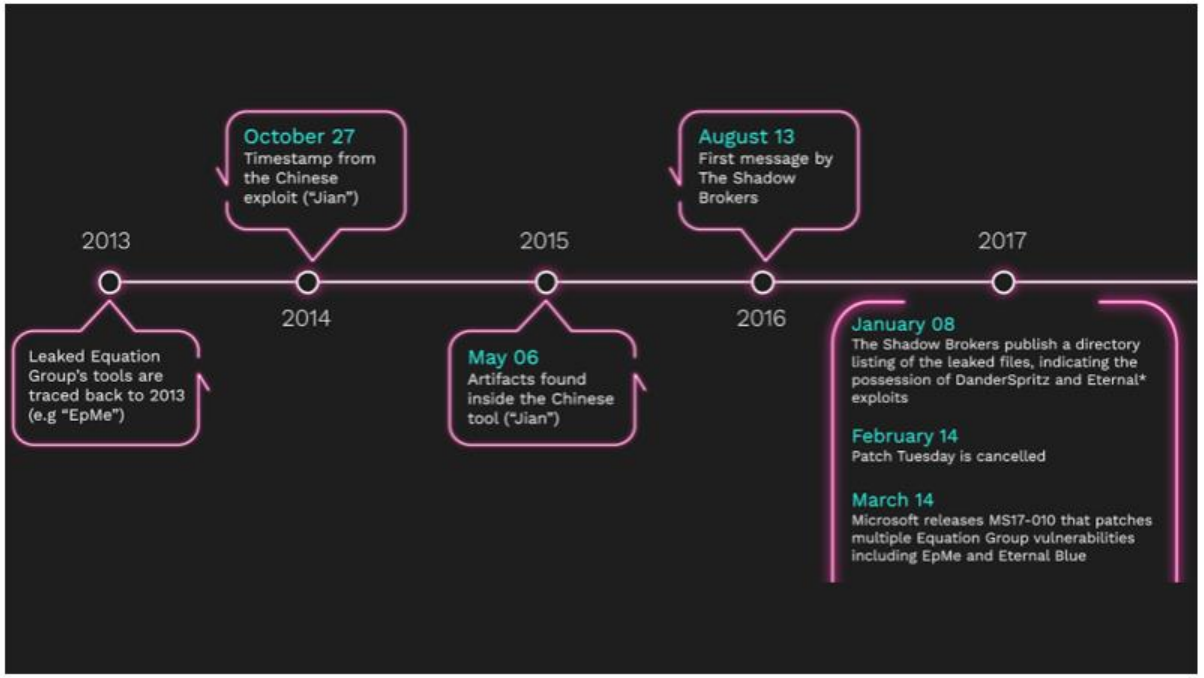
Computer System GmbH Ilmenau
Ackermannstraße 3
98693 Ilmenau
Tel.: +49 3677 6480-40
Fax: +49 3677 6480-55
h.langenhan@cs-ilmenau.de
www.cs-ilmenau.de
www.csi-technik.de

staatliche Überwachung wird ausgeweitet

l+f: Selbstbedienungsladen NSA

Offenbar hat eine chinesische Hacker-Gruppe Zero-Day-Exploits der NSA geklaut, lange bevor das die Shadow Broker getan haben.

Lesezeit: 3 Min. In Pocket speichern 49



EternalBlue – der NSA Exploit

EternalBlue wurde von einer Unterabteilung der US-amerikanischen NSA entwickelt.
Der Code vom Angriffswerkzeug wurde von der Shadow BrokerGruppe geleakt und bei den Angriffen **WannaCry** und **NotPetya** eingesetzt bzw. darauf aufgebaut.

staatliche Überwachung wird ausgeweitet

Vault 7: CIA Hacking Tools Revealed

WikiLeaks Leaks News About Partners

- FoxitReader Portable DLL Hijack
- Sophos Virus Removal Tool DLL Hijack
- Kaspersky TDSS Killer Portable DLL Hijack
- ClamWin Portable DLL Hijack
- Iperius Backup DLL Hijack
- OperaMail DLL Hijack
- Sandisk Secure Access v2 DLL Hijack
- LibreOffice Portable DLL Hijack
- BabelPad Portable Hijack
- Notepad++ DLL Hijack
- McAfee Stinger Portable DLL Hijack
- Skype Portable DLL Hijack
- Opera Portable DLL Hijack

staatliche Überwachung wird ausgeweitet

BSAFE

NSA bezahlte RSA Security, um Krypto-Backdoor einzusetzen

10 Millionen US-Dollar zahlte die NSA an das Sicherheitsunternehmen RSA Security, um Dual_EC_DRBG in seiner BSafe-Bibliothek als Standard einzusetzen. Bereits im September 2013 hatte RSA davor gewarnt, die Bibliothek zu nutzen.

21. Dezember 2013, 9:56 Uhr, Jörg Thoma

(Bild: RSA Security)

Das Unternehmen RSA warnt vor seinem eigenen Produkt BSafe.

staatliche Überwachung wird ausgeweitet

NETZPOLITIK.ORG

Automatisierte Anklage

China entwickelt „Staatsanwalt mit Künstlicher Intelligenz“

Chinesische Ermittlungsbehörden könnten künftig weitere digitale Unterstützung erhalten. Wissenschaftler:innen aus Shanghai haben ein System entwickelt, das gängige Straftaten erkennen und selbstständig Anklage erheben können soll.

30.12.2021 um 14:19 Uhr - Tomas Rudl - in Technologie - 17 Ergänzungen

Ermittlungsbehörden könnten in China bald weitere digitale Unterstützung erhalten. (Symbolbild)

Die Software könne mit 97-prozentiger Zuverlässigkeit Anklage erheben und sei auf die Erkennung der acht gängigsten Straftaten in Shanghai spezialisiert.

China exportiert diese Technologien in die ganze Welt.

staatliche Überwachung wird ausgeweitet

NETZPOLITIK.ORG

Kindergeldaffäre

Niederlande zahlen Millionenstrafe wegen Datendiskriminierung

Ein Skandal um rassistische Diskriminierung bei der Überprüfung von Kindergeldansprüchen erschüttert die Niederlande bis heute. Nun akzeptiert die Regierung ein Bußgeld in Millionenhöhe. Es ist der wohl erste Fall, bei dem eine Regierung für die automatisierte datenbasierte Diskriminierung von Bürger:innen zahlen muss.

29.12.2021 um 12:05 Uhr - Ingo Dachwitz - in Datenschutz - 6 Ergänzungen

Der Kindergeld-Skandal erschüttert die Niederlande bis heute

Das Vorgehen der Behörde hatte dabei erwiesenermaßen eine rassistische Prägung.

Wie die Datenschutzaufsicht in ihrer Pressemitteilung aufzählt, habe der Belastingdienst Daten über die Nationalität von Kindergeldbewerbern als Indikator für verschiedene Zwecke genutzt.

So sei etwa die Information, ob jemand eine doppelte Staatsbürgerschaft hat, in die Entscheidung über die Vergabe der Unterstützungsleistung eingeflossen, obwohl die Steuerbehörde diese Daten über mehr als 1,4 Millionen Menschen längst hätte löschen müssen.

staatliche Überwachung wird ausgeweitet

NETZPOLITIK.ORG

Subzero

Hacker-Behörde ZITiS prüft Staatstrojaner aus Österreich

Die Hacker-Behörde ZITiS ist mit der Firma DSIRF aus Österreich in Kontakt und lässt sich ihren Staatstrojaner „Subzero" vorführen. Ob deutsche Geheimdienste oder Polizeien den Trojaner haben und nutzen, verrät die Bundesregierung nicht mal dem Parlament.

03.12.2021 um 18:05 Uhr - Andre Meister - in Überwachung - 2 Ergänzungen

DSIRF verkauft Staatstrojaner und Gesichtserkennung. – Alle Rechte vorbehalten DSIRF

NETZPOLITIK.ORG

ZITiS

Deutschland und der Staatstrojaner Candiru

Über welche Staatstrojaner deutsche Behörden verfügen, will die Bundesregierung nicht verraten. Die Hackerbehörde ZITiS interessierte sich ab 2018 für Produkte des Herstellers Candiru. Laut der israelischen Zeitung Haaretz steht Deutschland auf der Kundenliste des Unternehmens.

23.12.2021 um 14:42 Uhr - Anna Biselli - in Überwachung - keine Ergänzungen

DSIRF, Quadream, Candiru

ZITiS interessierte sich nicht nur für Candirus Überwachungstechnologie, sondern sichtete Staatstrojaner mehrerer Unternehmen.

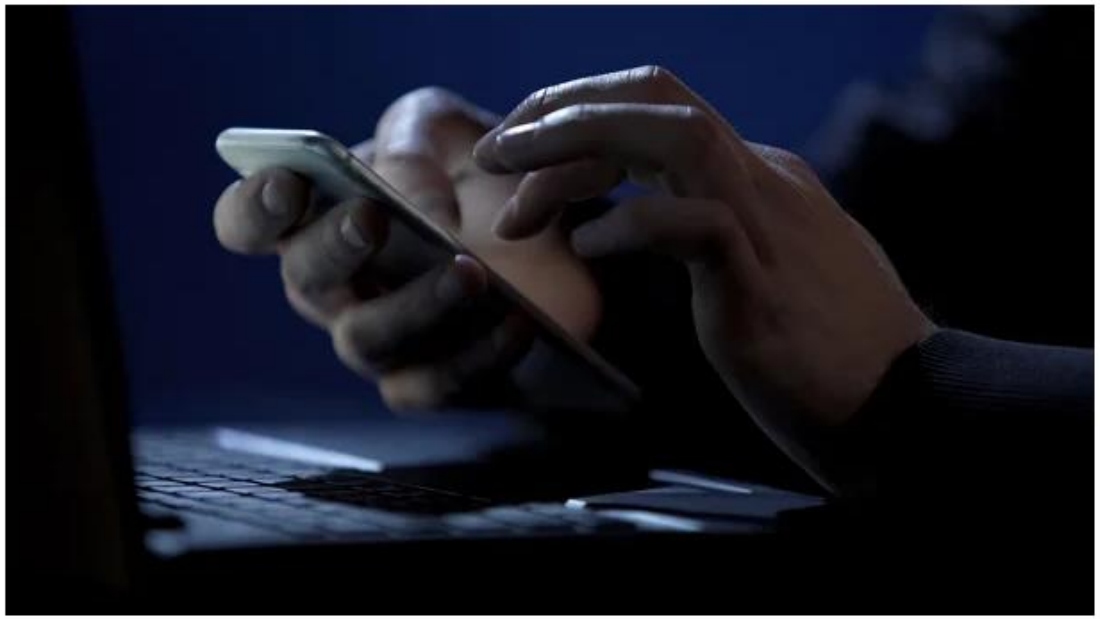
Aus früheren Anfragen wurde bekannt, dass dazu das Unternehmen DSIRF gehörte, das den Staatstrojaner Subzero vermarktet. Ebenso zog der Hersteller Quadream das Interesse der deutschen Hackerbehörde auf sich.

staatliche Überwachung wird ausgeweitet

Predator: iPhone-Spyware soll sich über Apples Kurzbefehle einnisten

Sicherheitsforscher haben neue Spyware auf dem iPhone eines ägyptischen Politikers analysiert. Das Gerät war zeitgleich mit der NSO-Spyware Pegasus infiziert.

Lesezeit: 2 Min. In Pocket speichern 38



(Bild: Shutterstock / Motortion Films)

20.12.2021 10:53 Uhr | Mac & i

Leider geil: NSOs Pegasus-Exploit für iPhone-Spyware enthüllt

Google hat den iMessage-Exploit analysiert, mit dem NSO iPhones von Menschenrechtlern und Journalisten in Wanzen verwandelte. Technisch ist er atemberaubend.

<u>Spyware-Problem reicht über einzelne Anbieter hinaus:</u>

Predator werde von der noch weitgehend unbekannten Firma Cytrox entwickelt, die unter anderem in Israel und Ungarn ansässig sei und Berichten zufolge zu Intellexa gehört.

Der Verbund beschreibe sich als "EU-basiert und reguliert" und wolle mit der NSO Group konkurrieren, wie Citizen Lab ausführt.

staatliche Überwachung wird ausgeweitet

NETZPOLITIK.ORG

Geheime Unterlagen: BND will 4,5 Millionen Euro für Zero-Day-Exploits ausgeben (Update)

09.11.2014 um 17:50 Uhr - Andre Meister - 2 Ergänzungen

Der aktuelle Spiegel berichtet:

> Geheimen Unterlagen zufolge hat der Bundesnachrichtendienst (BND) bis 2020 rund 4,5 Millionen Euro eingeplant, um auf dem grauen Markt Informationen über Software-Schwachstellen einzukaufen. Das berichtet der SPIEGEL in seiner aktuellen Ausgabe.

Staatliche Stellen sollten Sicherheitslücken schließen, nicht ausnutzen.

> Das Bundesamt für Sicherheit in der Informationstechnik (BSI) teilte auf Anfrage mit, es habe bis September 2014 einen Vertrag mit der französischen Firma Vupen unterhalten. Sie gilt als Weltmarktführer für Software-Schwachstellen. Zweck des Vertrags, so das BSI, sei „ausschließlich der Schutz der Regierungsnetze“ gewesen.

Warum ist Datenschutz notwendig?

Datenschutz ist notwendig zur freien Entfaltung der Persönlichkeit jedes Menschen

„Grundrecht auf informationelle Selbstbestimmung“
Schutz der Privatsphäre: Kenntnis darüber, welche Daten wo gespeichert sind. (Volkszählungsurteil vom 15.12.1983)

„Grundrecht auf digitale Intimsphäre“
Schutz der Daten in IT-Systemen sowie deren Vertraulichkeit und Integrität.

BUNDES-
VERFASSUNGS-
GERICHT

Die DSGVO schreibt vor…

Wann darf rechtmäßig verarbeitet werden?

Der Grundsatz gilt weiter: **Verbot mit Erlaubnisvorbehalt**

Artikel 6 Abs. 1:

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die Person hat ihre Einwilligung zu der Verarbeitung … für einen oder mehrere bestimmte Zwecke gegeben;
b) die Verarbeitung ist für die Erfüllung eines Vertrags, … die auf Anfrage der betroffenen Person erfolgen;
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt (andere Gestze);
d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, … überwiegen, insbesondere dann, wenn es sich … um ein Kind handelt.

Die DSGVO schreibt vor…

Grundregeln

Rechtsgrundlage:
Immer wenn personenbezogene Daten „angefasst“ werden, muss es dafür eine Rechtsgrundlage oder eine Einwilligung geben.

Daten beim Betroffenen erheben:
Wenn möglich, sind die Daten immer direkt beim Betroffenen zu erheben. Wenn nicht, ist er i. d. R. zumindest darüber zu informieren
(informationelle Selbstbestimmung).

Auskunftsrechte:
Der Betroffene muss jederzeit Kenntnis haben, dass und welche Daten über ihn gespeichert werden. Betroffener darf Auskunft verlangen! (Auskunftsrecht)
(Artikel 13 / 14 / 15 EU-DSGVO)

…

Die DSGVO schreibt vor...

...

Zweckbestimmung:
Erhobene Daten dürfen ausschließlich nur für den ursprünglich Zweck, für den sie erhoben wurden, verwendet werden.

(Artikel 5 EU-DSGVO Grundsätze für die Verarbeitung personenbezogener Daten)

Datensparsamkeit:
So wenig Daten wie nötig dürfen erhoben, verarbeitet und genutzt werden.

Berichtigung:
Fehler oder falsche personenbezogene Daten müssen berichtigt werden.

(Artikel 16 EU-DSGVO Berichtigung).

Schutz durch technische und organisatorische Maßnahmen:
Daten müssen vor Missbrauch, Beschädigung oder Verlust geschützt werden.

(Artikel 32 EU-DSGVO Sicherheit der Verarbeitung).

Weiter Gesetze schreibt vor...

IT-Sicherheitsgesetz 2.0

NIS 2.0

Die Norm **IEC 62443** - technischen Anforderungen der Industrienorm IEC 62443 an die Sicherheit und den störungsfreien Betrieb von Industrial Control Systems

§ 75B SGB V - Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragspsychotherapeutischen Versorgung

Gaia-X - ein Projekt zum Aufbau einer leistungs- und wettbewerbsfähigen, sicheren und vertrauenswürdigen Dateninfrastruktur für Europa

....

Fazit

Wie gehe ich als privater Unternehmer damit um?

Für eigene Informationssicherheit sorgen.

Die IT-Sicherheit als Kernprozess im Unternehmen betrachten.

Vertrauen zu Cloud-Systemen?

Vertrauen zu Geräten und Systemen (Software)?

Aktuelle Entwicklung Datenschutz und IT-Sicherheit

Fragen?

Vielen Dank für die Aufmerksamkeit!