

Update IT-Sicherheitsrecht

Dr. Florian Deusch

ANWALTSKANZLEI DR. GREYER

Prof. Dr. Tobias Eggendorfer

Agentur für Innovation in der Cybersicherheit GmbH

Herbstakademie 2022

Inhalte

- Gefährdungslage
- Geplante und aktuelle Rechtsakte (EU)
- Rechtsprechung und Verwaltungspraxis

Gefährdungslage

Automotive supplier breached by 3 ransomware gangs in 2 weeks

By **Sergiu Gatlan**

August 10, 2022

05:07 PM

0

Cyberangriff: IHK-Verbände weitgehend offline, auch telefonisch nicht erreichbar

Nach einem Cyberangriff auf die Industrie- und Handelskammern sind die weitgehend offline. An der Behebung werde gearbeitet, heißt es in sozialen Netzen.

Quellen: bleeping-computer.com, heise.de

Gefährdungslage

- Vermehrt Angriffe auf IT-Systeme
 - CyberWar Ukraine - Rußland
 - Ransomware
- Vergrößerte Angriffsfläche durch Corona & Homeoffice
- Weiterhin
 - unzureichend qualitätsgesicherte Software
 - Software-Monokultur
 - „Schlangenöl“
 - überschaubare Ermittlungserfolge

Geplante und aktuelle Rechtsakte (EU)

- NIS2 u.a.: Neue Sicherheitspflichten
- Chatkontrolle

NIS2 u.a. - Neue Sicherheitspflichten

- Branchenspezifisch (NIS2)
- Europäische Digitale Identität (eIDAS-VO)
- Plattformbetrieb (Digital Markets Act)
- eCommerce (Digital Services Act)
- Datenvermittlungsdienste (Data Governance Act)
- Funkanlagen und Maschinen

Chatkontrolle

- Vorschlag COM(2022) 209 & VO (EU) 2021/1232
- Ziel: Bekämpfen von Child Abuse
- Idee: Chats mitlesen
- Umsetzung: **Magie**
 - Nur relevante Chats mitlesen
 - Trotz Verschlüsselung
 - Nicht knackbar - außer für Regierung
 - Und nur für Child Abuse

Rechtsprechung und Verwaltungspraxis

- Disassemblierung (EuGH C13/20)
- Hackback und IT-Grundrecht
- Kryptohandys
- BSI-Warnung zu Kaspersky
- Geheimhaltungsmaßnahmen GeschGehG
- Sicherheit Online-Meetings (WebEx & Co)
- Fragen zur DSGVO

Disassemblierung / Dekompilierung

- EuGH Urt. v. 06.10.2021 - C-13/20
- „Dekompilieren“ als bestimmungsgemäße Nutzung
- Idee EuGH: Bugs selbst beheben
- Begriffe
 - Assembler, OpCode, Maschinencode
- Umsetzungsaufwand:

Beispiel

C-Code

```
#include <stdio.h>

int main ()
{
    unsigned int count = 0;
    count++;
    printf("%d\n", count);
    return 0;
}
```

Disassembliert

```
lea    0x4(%esp), %ecx
and    $0xffffffff0, %esp
pushl  0xffffffffc(%ecx)
push   %ebp
mov    %esp, %ebp
push   %ecx
sub    $0x24, %esp
movl   $0x0, 0xffffffff8(%ebp)
addl   $0x1, 0xffffffff8(%ebp)
mov    0xffffffff8(%ebp), %eax
mov    %eax, 0x4(%esp)
movl   $0x8048470, (%esp)
call   0x8048298 <printf@plt>
mov    $0x0, %eax
add    $0x24, %esp
pop    %ecx
pop    %ebp
lea    0xffffffffc(%ecx), %esp
```

ret

Hackback & IT-Grundrecht

- BVerfG, Urt. v. 26.04.2022 - 1 BvR 1619/17
- Hackback erfordert **bekannte** Sicherheitslücke
 - Bekannt: Dem Staat
 - Wem noch?
 - Geheimhaltungsaufwand ↔ Zweitentdeckung
- Weiteres Problem:
„Wir waren überrascht und vor allem entsetzt, daß diese Schnüffelsoftware nicht einmal den elementarsten Sicherheitsanforderungen genügt“
(CCC zu Bundestrojaner, 2011)

Kryptohandys

- EncroPhone / EncroChat
- Französische Behörden ermitteln gegen Dealer
- Einige Dealer nutzen EncroPhone
Konkreter Anteil: Streitig.
- Deutsche Behörden und BGH 5 StR 457/21:
EncroPhone-Nutzer = Dealer
- Problematisch:
Unschuldsvermutung ↔ hinreichender Tatverdacht

BSI-Warnung zu Kaspersky

- OVG Münster, Beschl. v. 28.04.2022 - 4 B 473/22
- Kaspersky „gehört“ russischen Staatsbürgern
- Rußland überfällt Ukraine, potentieller CyberWar
- Virens Scanner hat umfassende Zugriffsrechte
 - **Erforderlich** für Betrieb
 - Scan ist **gewünschte** Funktion
- BSI warnt vor Kaspersky Virens Scanner, weil
 - russisch
 - Zugriffsrechte
 - potentielle Backdoor

Schwierige Warnung vor Kaspersky

Stand: 05.08.2022 05:00 Uhr

Im März hatte das für IT-Sicherheit zuständige Bundesamt vor Antiviren-Software von Kaspersky gewarnt. Dokumente zeigen nun, wie schwer sich die Behörde bei der Entscheidungsfindung tat und wie eng das Innenministerium involviert war.

...

Nur zwei Stunden später reagiert der Präsident der Behörde, Arne Schönbohm, in einer internen E-Mail knapp und mit Tippfehler, wie man mit dem Schreiben von Kaspersky umgehen soll: "Glaube leider gar nicht antwortem".

Quelle: Tagesschau.de


Geheimhaltungsmaßnahmen

- OLG Schleswig-Holstein, Urt. v. 28.04.2022 - 6 U 39/21
- Geheime Informationen iSv § 2 Nr. 1b GeschGehG
 - Identifizieren
 - Kategorisieren
- Identifizieren und Bewerten der Schutzmaßnahmen
 - Need-to-Know
 - TOM
- TLS vs. „End-Zu-End“-Verschlüsselung

Sicherheit Online-Meetings

- LAG Köln, Beschl. v. 25.06.2021 - 9 TaBV 7/21
- Vertraulichkeit § 129 BetrVG a.F. / § 30 (2) Nr. 3 BetrVG n.F.

- LAG Köln: „alle marktgängigen Konferenzsysteme hinreichend sicher“

- 
- IT-Sicherheit: Zweifelhaft

- LAG Köln: Art. 44 DS-GVO nicht relevant für BR

Vermieter als TK-Anbieter

- BGH Urt. v. 18.11.2021 - I ZR 106/20
- TV-Anschluß durch Vermieter sei TK-Leistung bei mehr als 100.000 Mietern
- Konsequenz für Vermieter
 - IT-Sicherheitspflichten § 165ff TKG
 - Registrierung § 5 TKG
- Übertragbar: Arbeitgeber mit 100.000 Beschäftigten auch TK-Anbieter?

Fragen zur DSGVO

- Vorlage zum EuGH durch KG Berlin 3 Ws 250/21
- Bußgeld gegen Unternehmen?
(Art. 83 DSGVO ↔ §31 OWiG)
- IT-Sicherheit als Grund pers.-bez. Daten zu
verarbeiten?
(Generalanwalt beim EuGH C-77/21)
- TOM-Nachweis (Art. 32 DSGVO)
LG München I, 09.12.2021 31 O 16606/20
LAG BaWü, 25.02.2021, 17 Sa 37/20
- TOM unverzichtbar (DSK Beschluß)
- Geschäftsführer als Verantwortlicher
OLG Dresden, 30.11.2021 - 4 U 1158/21

Fazit

- Entscheidend für rechtliche Beurteilung:

Sachverhaltsermittlung



Wissenstransfer
Informatik ↔ Recht

Ihre Anmerkungen, Gedanken?

- **Dr. Florian Deusch**
ANWALTSKANZLEI DR. GRETTNER
deutsch@gretter-rae.de
www.gretter-rae.de

- **Prof. Dr. Tobias Eggendorfer**
Agentur für Innovation in der Cybersicherheit GmbH
eggendorfer@cyberagentur.de
www.cyberagentur.de / www.eggendorfer.info