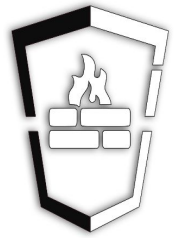


Panel zum IT-Sicherheitsgesetz v2.0

Panel zum IT-Sicherheitsgesetz v2.0

Teilnehmer: Teresa Ritter – Bitkom e.V.
Thorsten Schröder – CCC e.V.
Dr. Gerhard Schabhüser – BSI

Moderation: Johannes ‚ijon‘ Rundfeldt

Panel zum IT-Sicherheitsgesetz v2.0

- Alle Panel-Teilnehmer haben spannende, einzigartige Einblicke in Behörden, Wirtschaft und Community
- Alle Panel-Teilnehmer vertreten trotzdem ihre eigene Meinung und sprechen nicht offiziell für die Organisationen von denen sie kommen

Panel zum IT-Sicherheitsgesetz v2.0

- Wir sprechen über das IT-SiG 2.0, in der letzten veröffentlichten Version vom 27.03.2019
- Frühere und breitere Einbeziehung für solche Gesetze ist gewünscht.
- Nach der Ressortabstimmung ist eigentlich zu spät, um Stakeholder einzubeziehen.

Hackerparagraph-Erweiterung
§ 202e StgB

Verschärfung des Hackerparagraphens

- (1) Wer unbefugt ...

  einen Datenverarbeitungsvorgang oder einen informationstechnischen Ablauf auf einem informationstechnischen System beeinflusst oder in Gang setzt

  Wird mit Geldstrafe oder Freiheitsstrafe bis zu...

Hackerparagraph-Erweiterung
§ 202e StgB

Verschärfung des Hackerparagraphens

(3) Im Sinne dieser Vorschrift ist informationstechnisches System nur ein solches, das

zur Verarbeitung personenbezogener Daten geeignet oder bestimmt ist oder

Teil einer Einrichtung oder Anlage ist, die wirtschaftlichen, öffentlichen, wissenschaftlichen, künstlerischen, gemeinnützigen oder sportlichen Zwecken dient oder die den Bereichen Energie, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Versorgung, Haustechnik oder Haushaltstechnik angehört;

Hackerparagraph-Erweiterung
§ 202e StgB

Fragen:

- Fällt da nicht jeder Netzwerk-Scan drunter? - (nmap, nessus)
- Wie schützt sich ein Pentester, der von seinem Kunden 1000 IPs bekommt, von denen zwei versehentlich nicht mehr dem Kunden gehören, sondern einem anderen Unternehmen?
- Müsste man den Paragraphen entschärfen? Wenn ja, wie?

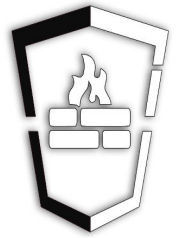
Hackerparagraph-Erweiterung
§ 202e StgB

Lösungsidee:

- Integrität und Vertraulichkeit eines informatischen Systems als Schutzgut in das StgB. Wird selbige erhalten, dann straffrei, wird selbige geschädigt, dann strafbar.

- Eine Änderung im gleichen Sinn dann auch für § 202c, §202f?

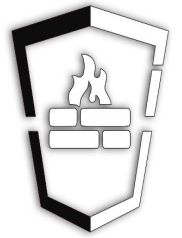
§ 126a – Zugänglichmachen von Leistungen zur Begehung von Straftaten



§126a StgB -

(1) Wer Dritten eine internetbasierte Leistung zugänglich macht, deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten zu ermöglichen, zu fördern oder zu erleichtern, wird mit Freiheitsstrafe bis zu … bestraft

§ 126a – Zugänglichmachen von Leistungen zur Begehung von Straftaten



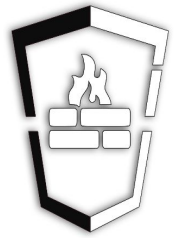
Fragen:

- TOR-Node betreiben?
- Öffentlichen VPN-Dienst betreiben?
- Cafébetreiber bietet anonymes WLAN an?
- Bestimmtheitsgebot?

§ 126a – Zugänglichmachen von Leistungen zur Begehung von Straftaten

(3) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer die Tat gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten im Sinne dieser Vorschrift verbunden hat, begeht.

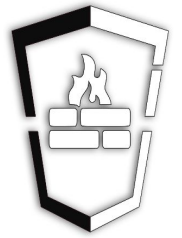
§ 126a – Zugänglichmachen von Leistungen zur Begehung von Straftaten



Fragen:

- Sorgfältiger Infrastrukturbetrieb benötigt doch immer ein Team aus Admins, oder?
- Kosten für den Betrieb (eines VPN-Gateways) auf die Teilnehmer umlegen und dabei minimal Gewinn mache, ist die strafverschärfende Gewerbsmäßigkeit gegeben?

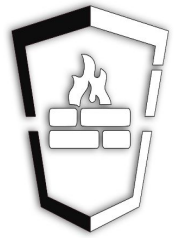
§ 126a – Zugänglichmachen von Leistungen zur Begehung von Straftaten



Lösung:

- Streichung?
- Konkreter Bestimmen was strafbar ist?
- ….?

Erzwungene Herausgabe von Online-Identitäten §163g StPO



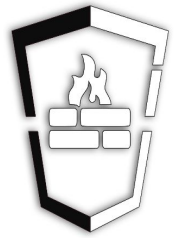
Begründen bestimmte Tatsachen den Verdacht, dass jemand Täter oder Teilnehmer einer Straftat im Sinne von § 100g Absatz 1 StPO ist, so dürfen die Staatsanwaltschaft sowie die Behörden und Beamten des Polizeidienstes auch gegen den Willen des Inhabers auf Nutzerkonten oder Funktionen, die ein Anbieter eines Telekommunikations- oder Telemediendienstes dem Verdächtigen zur Verfügung stellt und mittels derer der Verdächtige im Rahmen der Nutzung des Telekommunikations- oder Telemediendienstes eine dauerhafte virtuelle Identität unterhält, zugreifen. Sie dürfen unter dieser virtuellen Identität mit Dritten in Kontakt treten. Der Verdächtige ist verpflichtet, die zur Nutzung der virtuellen Identität erforderlichen Zugangsdaten herauszugeben. (...)

Erzwungene Herausgabe von Online-Identitäten §163g StPO

Fragen:

- Warum kein Richtervorbehalt?
- Welchen Nutzen hat dieser Paragraph für Behörden?
- Müssen auch TK-Anbieter die Zugangsdaten weitergeben?
- Was sollte man mit diesem Paragraphen tun?

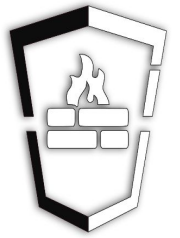
Responsible Disclosure



Fragen:

- Sollte man dem BSI gesetzlich untersagen, Sicherheitslücken zurückzuhalten?
- Sollte man allen Behörden gesetzlich untersagen, Sicherheitslücken zurückzuhalten?

Responsible Disclosure



Lösungsansatz: §7 (1) 2. BSIG

Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist. Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung von diese Produkte betreffenden Warnungen zu informieren. Diese Informationspflicht besteht nicht, wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird (...) Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken; ...

Responsible Disclosure

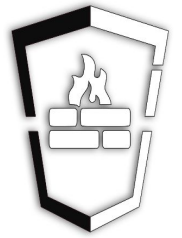
Lösungsansatz: §7 (1) 2. BSIG

Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist. Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung von diese Produkte betreffenden Warnungen zu informieren. ~~Diese Informationspflicht besteht nicht, wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird (...) Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken; ...~~

Infrastruktur in besonderem öffentlichem Interesse (ISBÖFI)

- „KRITIS-Pflichten“ nach §8a und 8b BSIG gelten auch für
- Anlagen die nicht von der Sektorliste §2 (10) BSIG abgedeckt sind
- Wenn das Unternehmen im Prime-Standard (DAX) ist
- Und Einvernehmen zwischen BMWI, BMJV, BMVI, BMVg, und BMU besteht
- Und Betreiber und Wirtschaftsverbände angehört wurden

Infrastruktur in besonderem öffentlichem Interesse (ISBÖFI)



- … zu diesen gehören (…) Infrastrukturen aus den Bereichen Chemie, Automobilherstellung, Rüstung und Kultur und Medien.
- An den Unternehmen (...) besteht wegen der volkswirtschaftlichen Bedeutung ein besonderes öffentliches Interesse.

Infrastruktur in besonderem öffentlichem Interesse (ISBÖFI)

Fragen:

- Warum der Paradigmenwechsel?
  - Vorher: „Infrastruktur deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde
  - Jetzt auch: „volkswirtschaftlichen Bedeutung“
- Warum ist „Rüstung“ dabei?
- Was tun? Sollte man eine Art „KRITIS light“ einführen und warum?

(vom BMI) unabhängiges BSI

Fragen:

- Was spricht dafür?
- Was spricht dagegen?

(vom BMI) unabhängiges BSI

Wie könnte man es machen?

1) Starke Unabhängigkeit – Modell BfDI
2) Fachliche Unabhängigkeit – Modell „statistisches Bundesamt“
3) Angliederung an BMWI
4) Angliederung an neu zu Schaffendes „Digitalministerium“

§9a BSIG – freiwilliges IT-Sicherheitskennzeichen

Fragen:

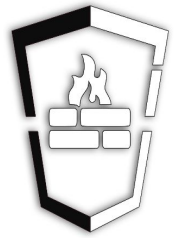
- Warum brauchen wir das?
- Ist es genug, das der Hersteller erklärt, das bestimmte IT-Sicherheitseigenschaften, wie z.B. die Einhaltung von BSI Technischen Richtlinien, vorhanden sind?
- Wird das BSI das Produkt prüfen, oder nur die Erklärung?
- Warum muss der Hersteller kein Exemplar des Produkts dem BSI zur Verfügung stellen?
- Wie könnte man es besser machen?

Hackback

Bisheriger Plan des BKA, sog. **5 Stufen Plan**

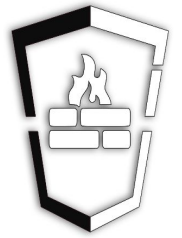
1) Hilfestellung leisten (Schutz, Absicherung), Angriff umlenken, blockieren, zurückverfolgen
2) In Systeme eingreifen, aus Ihnen Daten erheben, übernehmen, löschen, verändern
3) Maßnahmen vornehmen, die zu einer Überlastung, Nichtverfügbarkeit oder sonstigen Störung der Funktion [führen]
4) Maßnahmen 1-3 gegen Proxys des Angriff
5) Maßnahmen 1-4 ohne Wissen der betroffenen Person

Hackback



- Was spricht dafür, diese Befugnisse zu erteilen?
- Was spricht dagegen?
- Welche sollten nicht erteilt werden?

Hackback



Lösungsvorschlag

- Hackback „light“ - Bestimmungen aus §109a und b TKG „Daten- und Informationssicherheit“ und „Pflicht der Provider zur Meldung und Löschung“ erweitern
- Absatz 8 ist neu in IT-SiG 2.0
- Verschiedene vorhandene Verpflichtungen für Betreiber von Kommunikationsnetzen, Anordnungen des BSI oder der BnetzA in Bezug auf Löschen, Sperren, Umleiten von Traffic.
- Sehr ähnlich wie Maßnahme 1 und 2
- Anordnungsbefugnis (im Einvernehmen mit BSI und BnetzA) auch für BKA in Absatz 8 einpflegen