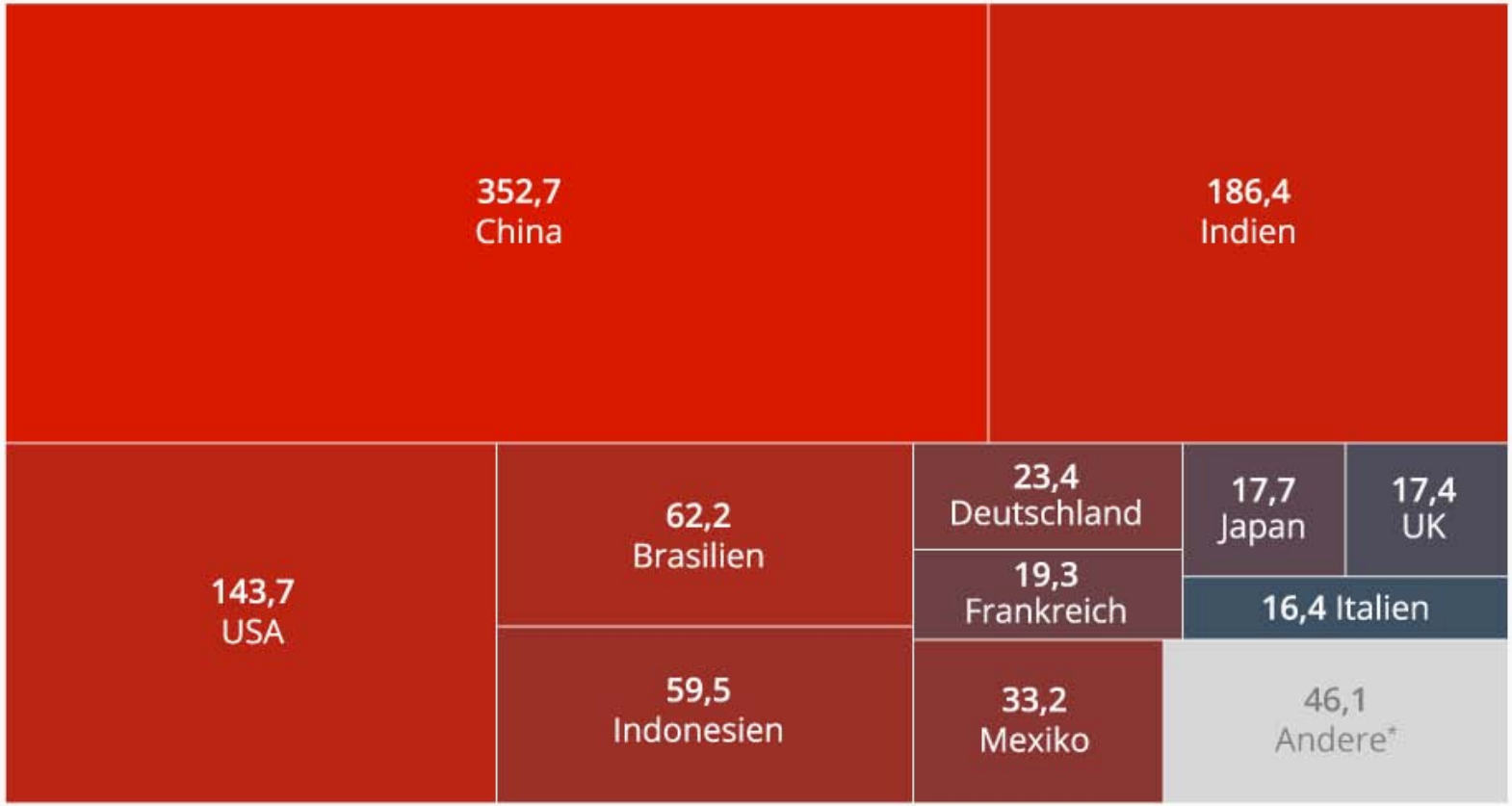
PLANET IC GmbH

IT- und Internetkompetenz für Wirtschaft und öffentlichen Sektor

23,4 Millionen deutsche Cyberkriminalitäts-Opfer

Anzahl der von Cyberkriminalität betroffenen Erwachsenen, 2017 (in Mio.)



* Australien, Kanada, Hong Kong, Niederlande, Neuseeland, Spanien, VAE
Basis: 21.549 Befragte (ab 18 Jahren) aus 20 Ländern; 05.–24.10.2017

Quelle: Symantec

statista

PLANET IC

Herzlich Willkommen

Digital - aber sicher: Überleben im Cyberkrieg!

www.planet-ic.de

PLANET IC

Herzlich Willkommen

Digital - aber sicher: Schritt für Schritt zu mehr IT-Sicherheit!

www.planet-ic.de

PLANET IC

Andreas Scher (Diplom-Informatiker)

- geschäftsführender Gesellschafter der PLANET IC GmbH
  (IT-Dienstleister mit 50 Mitarbeitern in Schwerin)
- Vorstandsmitglied der ITI-Initiative Mecklenburg-Vorpommern e.V.
  (regionaler IT-Branchenverband mit 60 Mitgliedern)
- Mitglied des IT-Ausschusses des Deutschen Industrie- und Handelskammertages in Berlin
- PLANET ist Mitglied in der Allianz für Cyber-Sicherheit Deutschlands
  (Initiative des Bundesamtes für Sicherheit in der Informationstechnik)

Wie werden PLANET und deren Kunden gestört oder angriffen?

SPAM

- kostet Rechenleistung, Arbeitszeit, …
- „interner SPAM“ (unbewusster „Innentäter“, technische Systeme)

Viren in eMails und Websites

- der Klassiker
- nicht nur von „fragwürdigen“ Websites

Ausnutzen von Bugs in der Software von Webservern & Anwendungen

- häufig PHP-basierte Systeme: Typo3, Wordpress, Drupal, Magento
- danach meist als Spammer aktiv

DDoS - Distributed-Denial-of-Service-Attacken

- CPU in die Knie zwingen, Speicher dicht machen
- Leitung ausmaxxen

Warum werden PLANET und deren Kunden angegriffen?

Kapern von Systemen als Sprungbrett

- um den Herkunftsort des Angreifers zu verschleiern

Kapern von Systemen, damit diese als BOT (Roboter) arbeiten

- um diese als Botnet andere Systeme angreifen zu lassen

Ausspähen von Nutzerdaten

- häufig verwenden Nutzer im Internet das gleiche Passwort, es reicht ein System
- Ausspähen von Kreditkartendaten

Erschleichen von Rechenleistung

- aktuell beliebt: Minen von Cryptowährungen

Weil man es kann!

- Scriptkiddies probieren aus, was geht
- Tools gibt es ausreichend

Warum werden PLANET und deren Kunden angegriffen?

Verschlüsseln von Daten

- um Geld für die Herausgabe zu erpressen
- Ransomware (Ransom - Lösegeld)

Kapern von Systemen, Anmeldung des Nutzers verhindern

- um Geld für die Herausgabe zu erpressen
- Ransomware (Ransom - Lösegeld)

Kapern von Telefonanlagen

- teure Auslandstelefonate umgehen

Angriff, um Systeme zu überlasten

- um Geld zu erpressen

Angriffe #1

```
[SNORT] vfw1.d11503.qvm.p4.net daily report

Events between  01 18 06:25:14  and  01 19 06:25:00
Total events: 22471
Signatures recorded: 101
Source IP recorded: 2700
Destination IP recorded: 501


Events from same host to same destination using same method
=============================================================================
 # of  from             to               method
=============================================================================
 1000  46.166.185.90    195.98.196.203   ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM
 1000  46.166.185.90    195.98.196.203   ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt
 1000  46.166.185.90    195.98.196.203   ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access
  681  91.247.38.57     195.98.196.92    ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT
  481  87.188.152.91    213.254.33.51    (ftp_telnet) Invalid FTP Command
  254  195.98.201.173   195.98.196.102   WEB-MISC apache directory disclosure attempt
  249  1.63.25.196      195.98.196.170   FTP format string attempt
```

Angriffe #2

```
[SNORT] vfw2.d11503.qvm.p4.net daily report

Events between  01 18 06:48:12  and  01 19 04:56:11
Total events: 59
Signatures recorded: 2
Source IP recorded: 6
Destination IP recorded: 4


Events from same host to same destination using same method
=============================================================================
 # of  from             to               method
=============================================================================
   18  172.16.1.7       195.98.208.4     COMMUNITY SIP TCP/IP message flooding directed to SIP proxy
   12  195.98.208.4     172.16.1.7       COMMUNITY SIP TCP/IP message flooding directed to SIP proxy
   12  172.16.1.36      195.98.208.4     COMMUNITY SIP TCP/IP message flooding directed to SIP proxy
```

Anforderungen & Herausforderungen

gesetzliche und oder branchenspezifische

- Bundesdatenschutzgesetz, Landesdatenschutzgesetz, Telemediengesetz, Telekommunikationsgesetz
- EU-Datenschutzgrundverordnung (mit Auswirkungen auf verschiedenste Gesetze)
- Kritis/IT-SiG, MaRisk (Mindestanforderungen an das Risikomanagement / BaFin), ...

interne

- Geld, Zeit, Mitarbeiter (immer zu wenig vorhanden), Patches?
- Mitarbeiter (als „unabsichtliche“ Täter, als Betroffene)
- Geschäftsführung

externe

- technische Entwicklung
- Geschäftspartner (Kunden, Lieferanten)
- IT-Dienstleister

Lösungsansätze

100-prozentige Sicherheit gibt es nicht

- man muss kommunizieren und interagieren
- Ressourcen stehen nicht beliebig zur Verfügung
- irgendwann wird irgendwas passieren

Realistische Risikoeinschätzung

- stufenweise, beginnend bei den Kernprozessen
- gemeinsam mit der Geschäftsführung

Realistischer Maßnahmenplan

- Budget aufstellen
- Maßnahmen sortieren
- nach geeigneter Zeit prüfen, überarbeiten

PLANET IC

Links & Kontakte

https://www.sicher-im-netz.de/

https://www.allianz-fuer-cybersicherheit.de/

https://www.bsi.bund.de

https://www.cert-bund.de/overview

http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/

LKA Mecklenburg-Vorpommern, +49 3866 64 4545, cybercrime.lka@polmv.de

Kriminalpolizeiinspektion Schwerin, +49 385 5180 0, kpi.schwerin@polmv.de

Vielen Dank für Ihre Aufmerksamkeit

Ihr Ansprechpartner

Andreas Scher
Telefon 0385 30 200 101
scher@planet-ic.de

PLANET IC GmbH
Mettenheimer Straße 9-15
19061 Schwerin

www.planet-ic.de