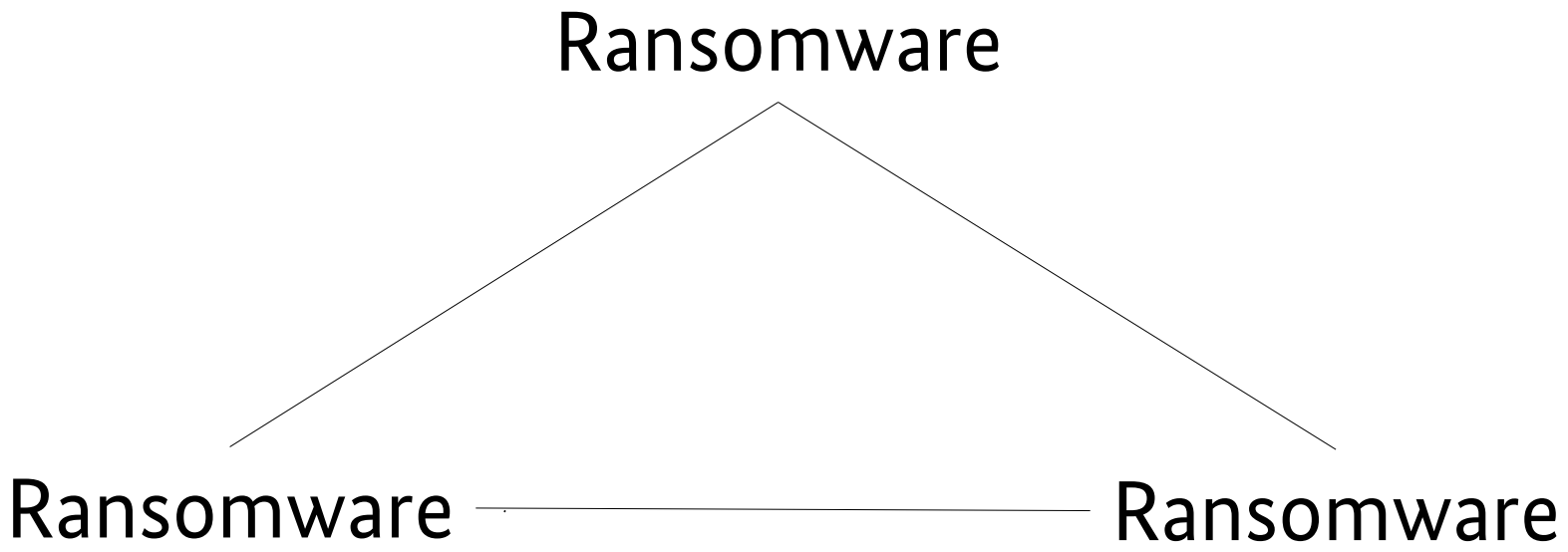
Bundesamt
für Sicherheit in der
Informationstechnik

Aktuelle Aspekte der Bedrohungslage in Bezug auf die Lieferkette

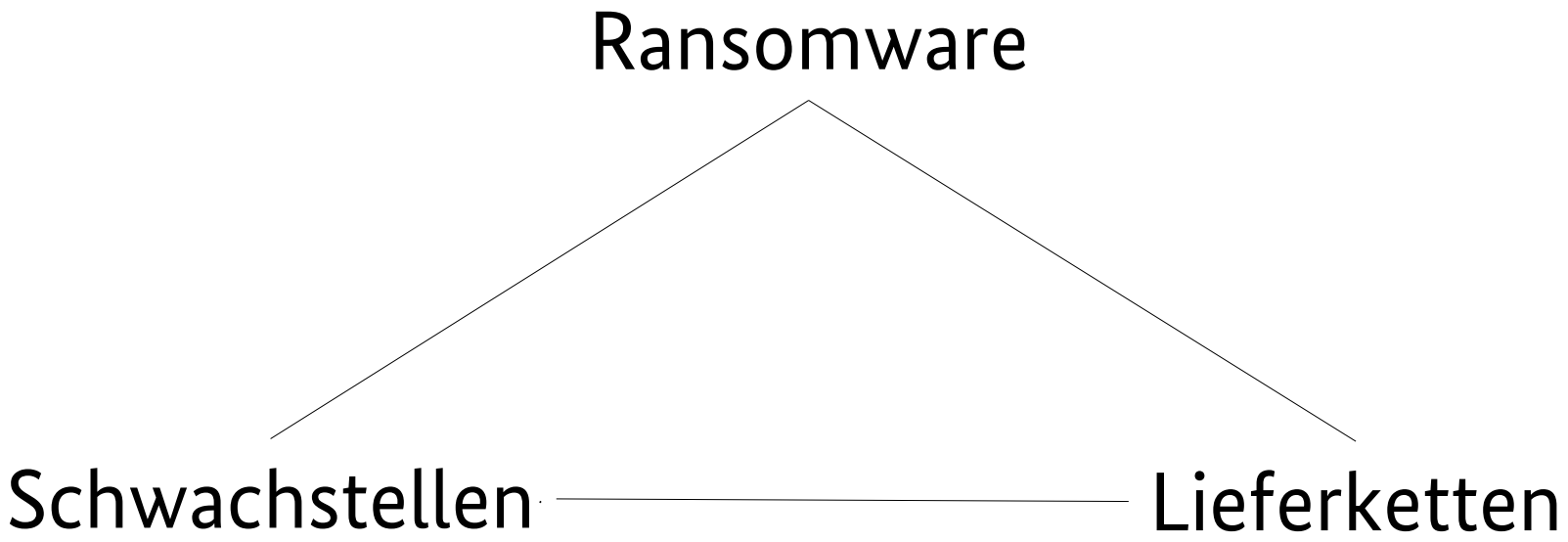
Isabel Münch
Fachbereichsleiterin IT-Sicherheitslage

17.03.2022, GI-Fachgruppe SECMGT

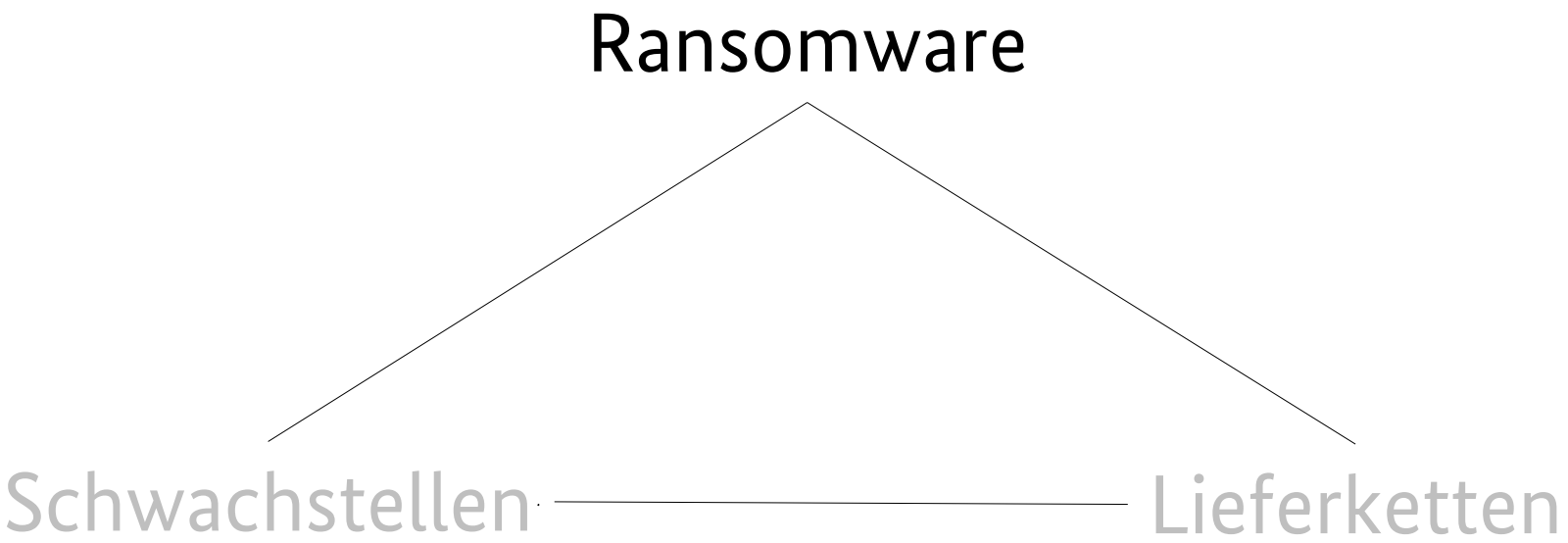
Die „Drei Top-Bedrohungen“



Die „Drei Top-Bedrohungen“



Die „Drei Top-Bedrohungen“



Ransomware – Schlagzeilen aus Deutschland

Uniklinik Düsseldorf: Ransomware "DoppelPaymer" soll hinter dem Angriff stecken

CYBER-KRIMINELLE LEGEN BETRIEB LAHM

Hacker-Angriff auf Verpackungsspezialist Optima in Schwäbisch Hall

Riesenprobleme bei Miltenyi Biotec in Teterow: Insider sprechen von Hacker-Angriff

Cyber-Attacke auf Saarbrücker Flughafen

Zeitungsproduktion gestört

Funke Mediengruppe wurde mit Erpressungstrojaner angegriffen

Software AG Opfer von Clop-Ransomware Attacke

KASEYA

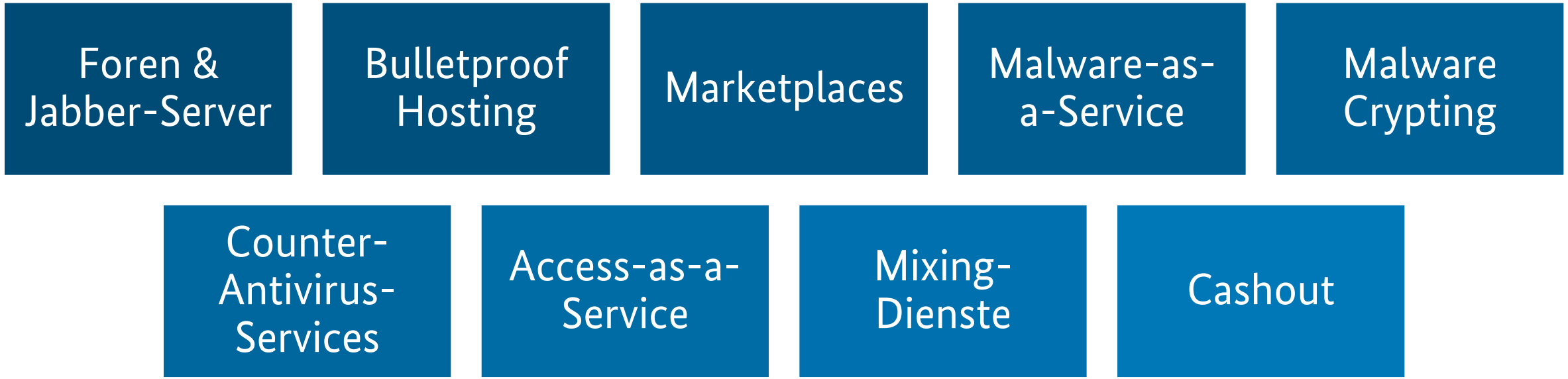
Was über Ransomware-Betroffene in Deutschland bekannt ist

Ein großer Ransomware-Angriff hat Hunderte Unternehmen weltweit getroffen. Auch deutsche Firmen sind darunter, manche hatten aber offenbar Glück.

NACH CYBERANGRIFF AUF ANHALT-BITTERFELD

Spekulationen um Name der Hackergruppe - „Pay or Grief“ soll hinter Lösegeldforderung stecken

Cybercrime-as-a-Service, das Cybercrime-Ökosystem



Quelle: angelehnt an Bundeslagebild Cybercrime 2019, BKA

Bundesamt für Sicherheit in der Informationstechnik

Big Game Hunting

Bundesamt für Sicherheit in der Informationstechnik

Ransomware

- Aktuell die **größte operative Bedrohung** der Cyber-Sicherheit
- Qualität steigt stetig
- Angriffe mit hoher Agilität
- Wirtschaftsmodell mit Arbeitsteilung: Ransomware-as-a-Service (RaaS)
- Big Game Hunting: Trend zu gezielten Angriffen auf Unternehmen
- Neue Kampagnen exfiltrieren Daten, verschlüsseln und erpressen, zusätzlich unter Androhung die Daten zu veröffentlichen
- BSI rät grundsätzlich von Zahlungen ab
- Eigene Betroffenheit? – „**Keine Frage des OB, sondern des WANN!**“

Bundesamt für Sicherheit in der Informationstechnik

Konsequenzen für Sie:

Wiederherstellungsaufwand der **wichtigsten** Verfahren:

>23 Tage

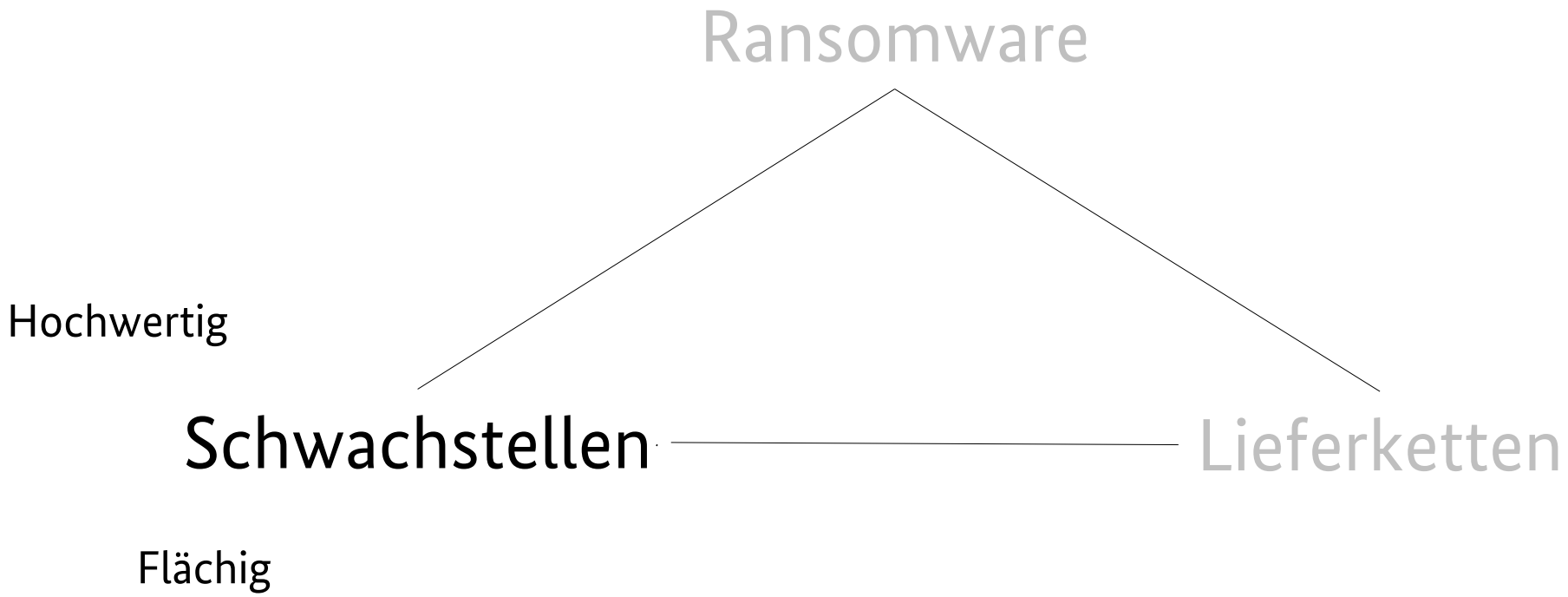
„vollständige“ Wiederherstellung:

Wochen – Monate bei ca. 1,85 Mio$

Nach: SOPHOS

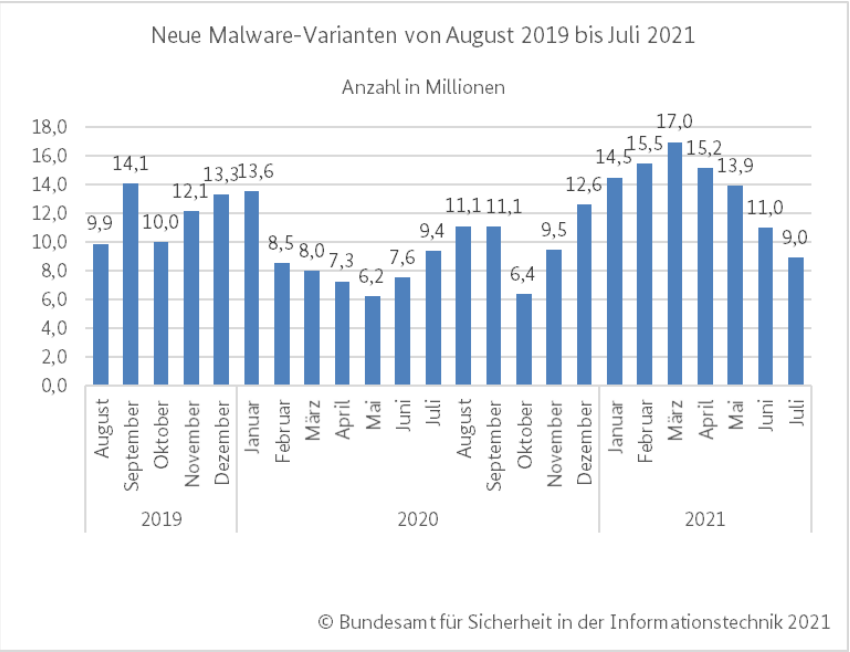
Bundesamt
für Sicherheit in der
Informationstechnik

Die „Drei Top-Bedrohungen“



Bundesamt
für Sicherheit in der
Informationstechnik

Schwachstellen & Malware

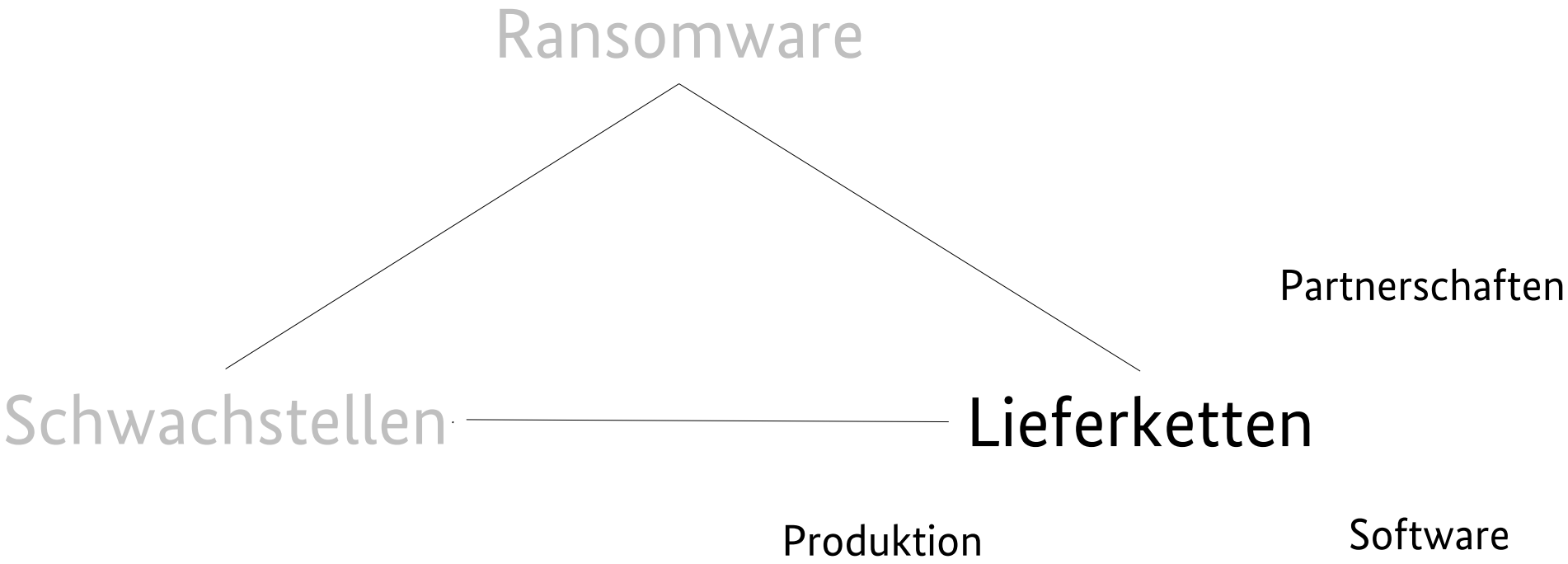


- **Schwachstellen als Einfallstor** für Angriffe (vgl. Emotet)
- Malware weiterhin eine der größten Bedrohungen
- Steigende Malwarezahlen = Steigendes Infektionsrisiko
- Herkömmliche signaturbasierte Detektion nicht ausreichend
- Juli 2021: Täglich durchschnittlich 289.000 neue Malware-Varianten
- **Kritikalität zunehmend** (vgl. Exchange, SolarWinds)
- **Maßnahmen:**

  - ✓ Patchen, Aktuell halten
  - ✓ Sicherheitsmaßnahmen konsequent umsetzen
  - ✓ Mitarbeiter sensibilisieren

Bundesamt für Sicherheit in der Informationstechnik

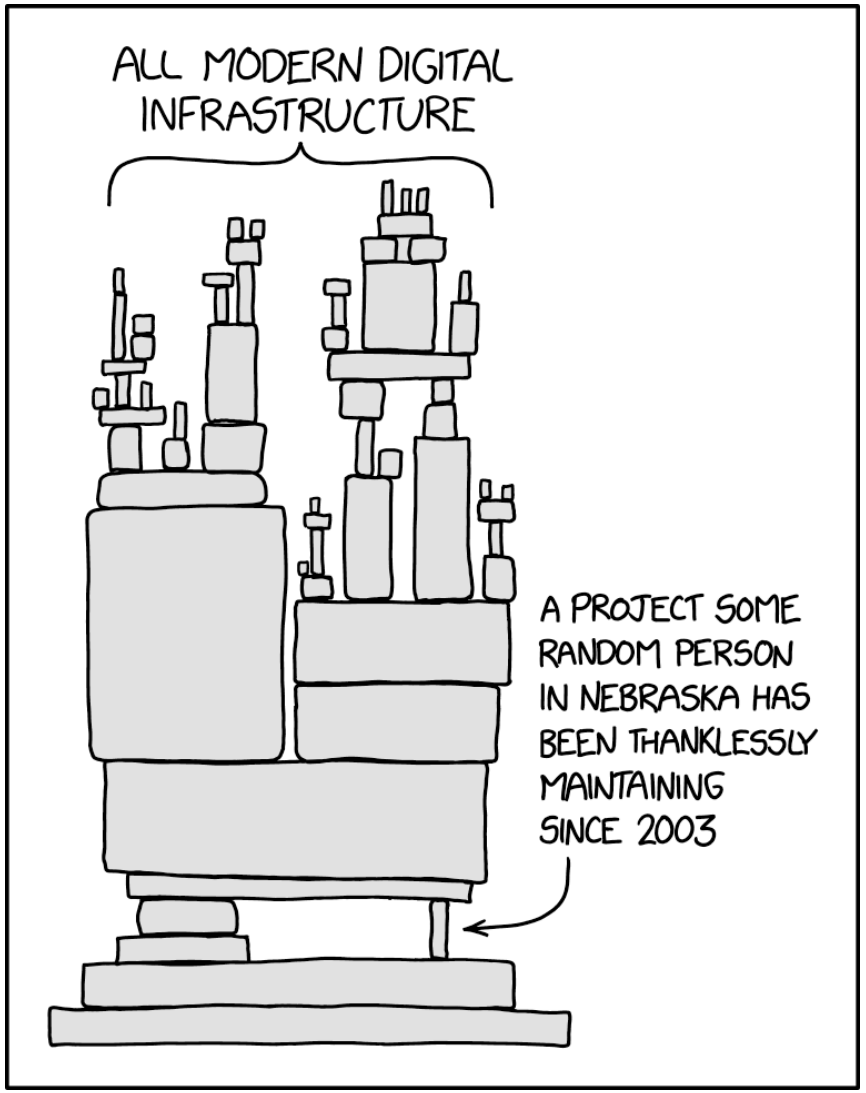
Die „Drei Top-Bedrohungen“



Bundesamt für Sicherheit in der Informationstechnik

https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
https://de.wikipedia.org/wiki/TISAX
https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

Supply-Chain - Herausforderung



https://xkcd.com/2347/

Supply-Chain-Angriffe

- **Steigende Abhängigkeit und Vernetzung** der IT-Infrastrukturen
  (vgl. Automotive)
- Ausfall oder Beeinträchtigung von Diensten des Unternehmensnetzes haben schnell **fatale und finanzielle Folgen**
- Cyber-Angriffe qualitativ immer ausgereifter und zielgerichteter (Fortschrittliche Angriffe)
- Angriffe häufig am Wochenende, um frühzeitige Entdeckung zu verhindern
- Office-IT-Netzwerke und Fernzugriffe als Einfallstor (Dienstleister, Home Office)
- **Auch Software-Lieferketten betroffen** (vgl. Kaseya, NotPetya)
- **Digitalisierung sicher und ganzheitlich umsetzen**

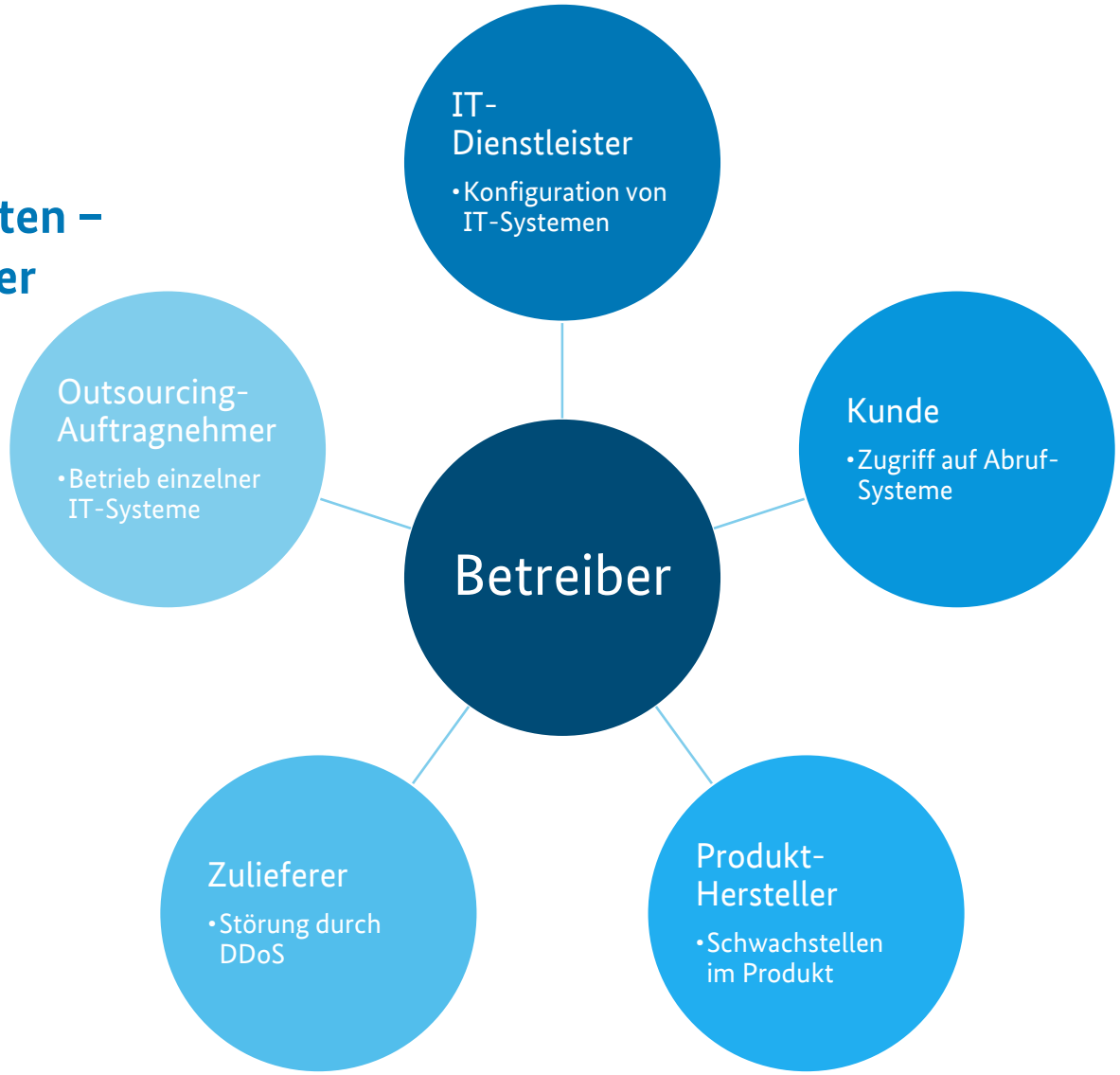
Varianten von Supply-Chain-Angriffen

- Supply-Chain-Angriffe auf IT = Cyber-Angriffe auf IT-Komponenten, die Teil der IT-Lieferkette einer IT-Umgebung sind
- Ziel: Manipulation von IT als Startpunkt für Cyber-Angriffe
- **Beispiele:**
- Kaseya
- SAP
  - Schwachstelle in SAP "CVE-2021-38178" mit CVSS-Score von 9.1/10
  - nach Änderung von Code auf einem System können die nachfolgenden Systeme ebenfalls mit dem geänderten Code versorgt werden
  - SAP hat mit SNOTE 3097887 Update bereitgestellt

- Supply-Chain-Angriffe über IT = Supply Chain Disruptions = Cyber-Angriffe auf Akteure in der Lieferkette (Produktion, Dienstleister)
- Wirkung (nicht immer Ziel): Stockungen in der Lieferkette / der Produktion
- **Beispiele:**
- Ransomware-Angriff auf Teile-Hersteller in der Automobil-Industrie
- DDoS-Angriff auf Zulieferer für Impfstoffproduktion

Lieferkette

komplexe Versorgungsketten –
nicht 3, sondern 100 Glieder



Bundesamt für Sicherheit in der Informationstechnik

Herausforderungen Lieferkette

- Information aller Stakeholder: Kunden und Kettenpartner
- Meldepflichten / Kontakt mit Behörden
  - Hilfe wird erwartet, aber nicht gesucht!
- Identifizierung der Teileproduzenten und –logistik inkl. der jeweiligen Versorgungsketten
  - Immer wieder: schwierig und langwierig
  - Versorgungsketten häufig nicht dokumentiert -> Auswirkungen von Produktionsausfällen oder Problemen nicht bekannt
  - Keine Kontakte etabliert
  - Liste der Dienstleister und Zulieferer, samt Priorisierung
  - Informationspakete
- klare Struktur der Zusammenarbeit, klare Aufgabenverteilung und Entscheidungs- und Weisungskette

Komplexität

- Häufig geben Produzenten Teile der Produktion oder sogar die gesamte Produktion an Dienstleister ab
- Zusätzlich zu betrachten: Hersteller von Maschinen, Verbrauchsgütern und Rohstoffen plus IT-Hardware und Software
  - In einigen Branchen werden große Netzwerke aus verschiedenen Dienstleistern und Partnern für ein und das selbe Produkt geknüpft -> Überschneidungen: Unique Selling Points führen zu Single Point of Failure
  - Abhängigkeit von Dienstleistern häufig nicht im Vorfeld bekannt, auch nicht Konkurrenzsituationen zwischen Kunden
- Verteilte Produktion benötigt Logistik
  - jeder Produzent und jeder seiner Dienstleister hat eigene Logistik
  - Auswahl und Verteilung von Lägern
  - Angriff auf Logistik-DL mitbetrachten!

Prävention

- 1-tägiger Workshop
  - ISB, Fachabteilungen und Sicherheitsexperten
  - Diskussion der Sicherheitsarchitektur, Sichtung auf größere Schwachpunkte und auf aktuelle
- Minimal-Notfallansatz
  - 1 Tag Kick-off/Planbesprechung
  - 5 Tage Audit
  - 2 Tage Aufstellen eines Maßnahmenplans
  - monatlicher, gemeinsamer JF zur Umsetzung
- Notfallmanagement / BCM
  - BSI-Standard 200-4

Prävention

- Patchen
- Backup
- Patchen
- Backup
- Patchen
- Backup
- **Grundlegende Sicherheit herstellen (z.B. IT-Grundschutz)!**

+ Dokumentation (Kenne deine Lieferkette!)

- Austausch mit anderen in der Lieferkette
  - International
  - In der Branche
  - Mit IT-Sicherheitsexperten

Fazit:
Ransomware-Abwehr hilft Ihrer gesamten IT-Sicherheit

Es ist keine Frage des **OB**, sondern eine Frage des **WANN!**

Sie wissen was passieren kann und Sie sind mitverantwortlich!

Es gibt viel zu tun - Fangen Sie JETZT an!

Was brauchen Sie denn noch? Die Fälle sind öffentlich, die Schäden bekannt ...
Jetzt investieren ist billiger, als wochenlang eingeschränkt zu sein und neu aufzubauen.

Wenn Sie glauben, bereit alles getan haben – nicht darauf ausruhen, lieber regelmäßig checken und aktualisieren

Bundesamt für Sicherheit in der Informationstechnik

BSI Good Practice Sammlung (Auszug)

zur Sensibilisierung und Vorfallsunterstützung

Hintergrundinformationen Ransomware, Sensibilisierung

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_**Managementabstract-Angriffe**.html
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/**Themen/Ransomware**.pdf

BCM Vorbereitung, BIA-Prozesspriorisierung

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/**bsi-standard-200-4_Business_Continuity_Management**_node.html

Notfallmanagement, Krisenstabsarbeit:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/**Standard_200-4_Bewaeltigung**.pdf
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/**Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall**.pdf

Mitarbeiter-Hilfen (Spin-off aus Wahlsicherheit):

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/**Infos-fuer-Kandidierende**/Info-fuer-Kandidierende/kandidierende_node.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/**Leitfaden-Kandidierende**.html

Bundesamt für Sicherheit in der Informationstechnik

Lieferketten- Aspekte
https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
https://de.wikipedia.org/wiki/TISAX

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Isabel Münch
Fachbereichsleiterin IT-Sicherheitslage
isabel.muench@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik