
CAAS – CYBER-CRIME AS A SERVICE
MAGENTA SECURITY KONFERENZ
08. MÄRZ 2018
THOMAS KÖNIGSHOFEN

AGENDA

- CaaS: Definitionen und Abgrenzungen
- Bedrohungspotenzial
- Beschaffung der Tools
- Typische Angebote und Geschäftsmodelle
- Gegenmaßnahmen

Quelle: CaaS analysis report. Y. Zheng A. Chaudhry

CAAS – DEFINITIONEN UND ABGRENZUNGEN

SaaS → Software as a Service
PaaS → Platform as a Service
CaaS → Crime as a Service; Cyber-Crime as a Service

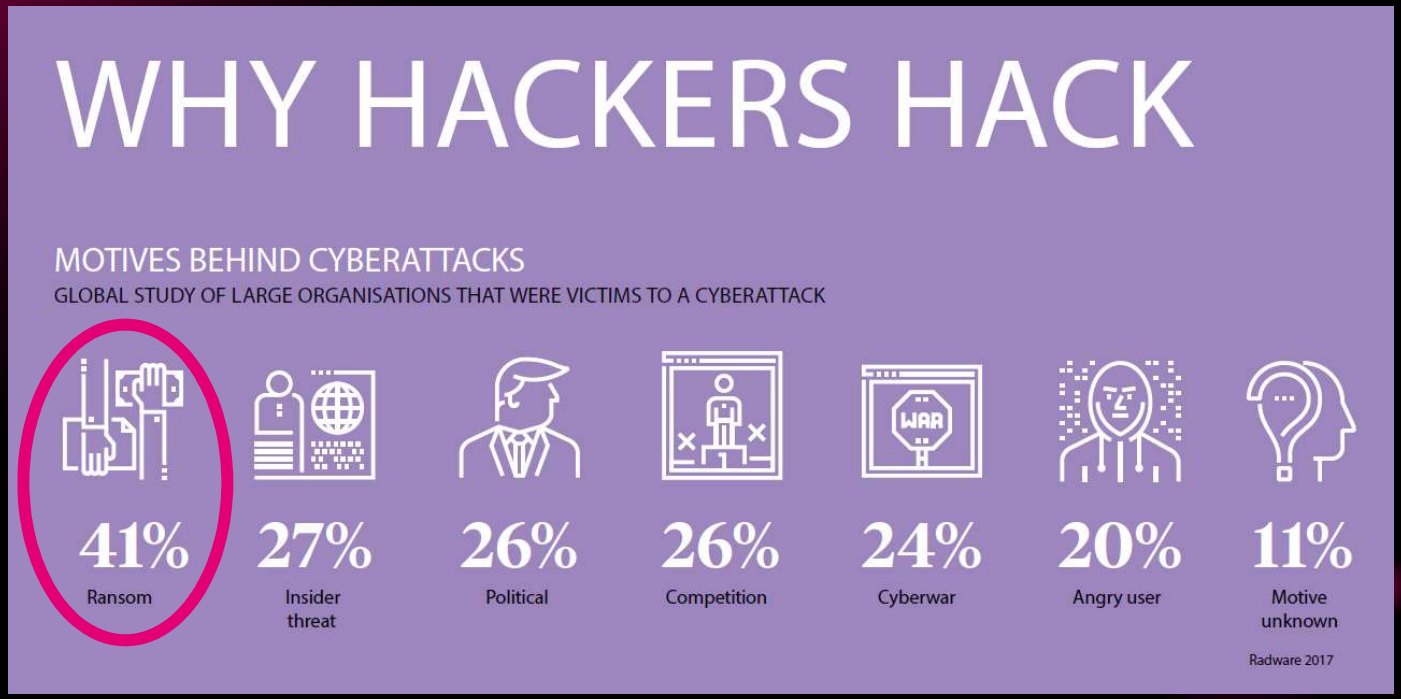
CRIME AS A SERVICE:

Das Dienstleistungsangebot an Dritte, gegen Bezahlung Straftaten zu begehen.

Cyber-Crime as a Service:

Das Dienstleistungsangebot an Dritte, gegen Bezahlung computergestützte Straftaten zu begehen oder dabei zu unterstützen

CYBERCRIME – DAS BEDROHUNGSPOTENZIAL



CYBERCRIME – DAS BEDROHUNGSPOTENZIAL

Fast 55 Milliarden Euro Schaden pro Jahr

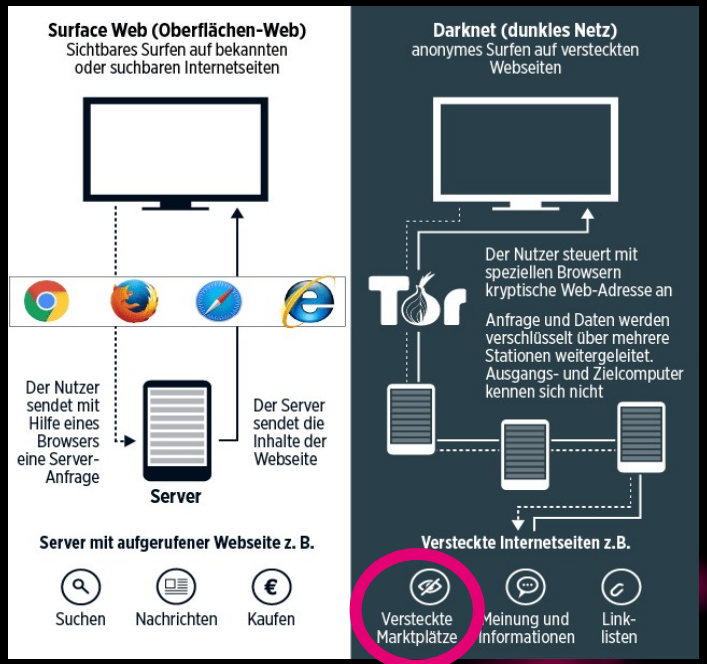
bitkom

Schäden in Deutschland in Milliarden Euro (Basis: Selbsteinschätzung)

	Schadenssummen in Mrd. Euro
Kosten für Ermittlungen und Ersatzmaßnahmen	21,1
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	17,1
Patentrechtsverletzungen (auch schon vor der Anmeldung)	15,4
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	15,4
Kosten für Rechtsstreitigkeiten	11,0
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	10,5
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	6,9
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	6,4
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	1,3
Sonstige Schäden	4,5
Gesamtschaden innerhalb der letzten 2 Jahre	**109,6**

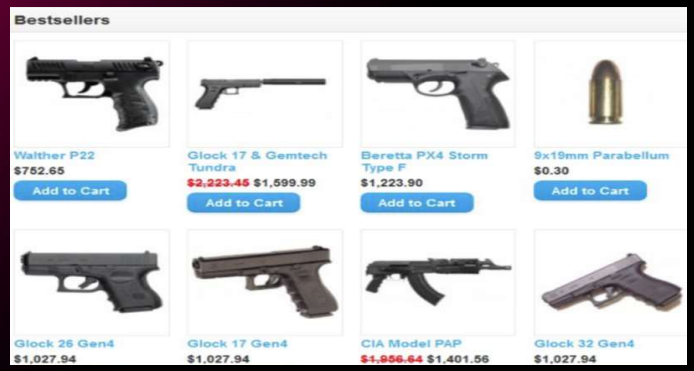
CYBERCRIME AS A SERVICE– BESCHAFFUNG

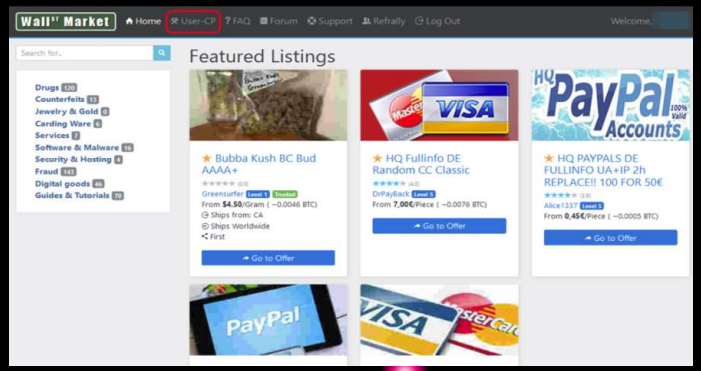
Quelle: freepik.com

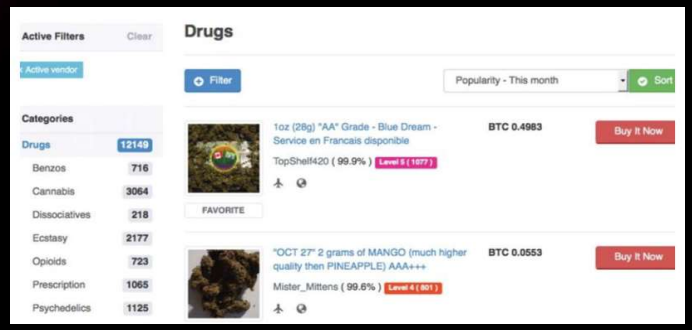


Quelle: info.BILD.de // Bundesregierung, Kompetenzzentrum öffentliche IT, dpa

CYBERCRIME AS A SERVICE– BESCHAFFUNG





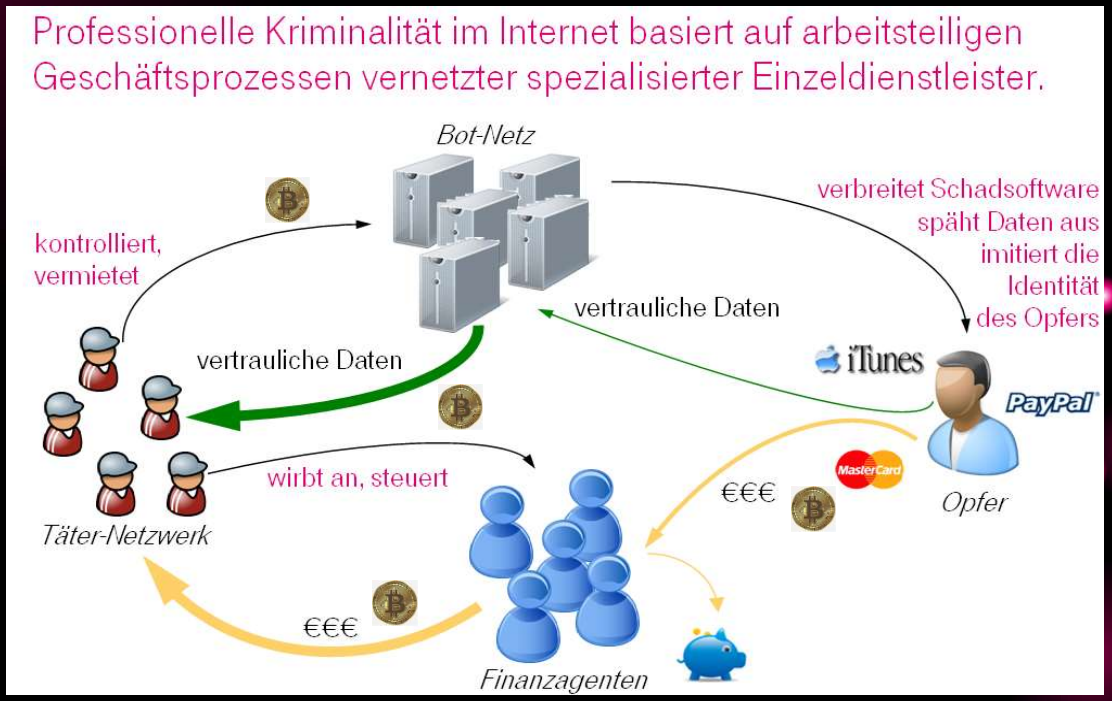


CYBERCRIME AS A SERVICE– TYPISCHE ANGEBOTE

- Ransomware (-toolkits)
- Bereitstellung von Botnetzen für verschiedene kriminelle Aktivitäten
- DDoS-Attacken
- Malware-Herstellung und -Verteilung
- Datendiebstahl
- Verkauf/Angebot sensibler Daten, z. B. Zugangs- oder Zahlungsdaten
- Vermittlung von Finanz- oder Warenagenten
- Kommunikationsplattformen zum Austausch von kriminellem Know-how, wie beispielsweise Foren
- „Infection on Demand“ (Verteilung von Schadsoftware auf Anforderung/Abruf)
- Anonymisierungs- und Hostingdienste zum Verschleiern der eigenen Identität
- Test-Portale zum Testen der Schadsoftware auf Detektierbarkeit durch Sicherheitsprodukte
- „Dropzones“ zum Ablegen illegal erlangter Informationen bzw. Waren

CAAS – TYPISCHE GESCHÄFTSMODELLE

Professionelle Kriminalität im Internet basiert auf arbeitsteiligen Geschäftsprozessen vernetzter spezialisierter Einzeldienstleister.



CAAS – ZU ERWARTENDE TRENDS

Einzeltäter spezialisieren sich

Täter schließen sich zu Netzwerken zusammen

Täter-Netzwerke bekommen Strukturen der OK

Klassische OK bedient sich Täter-Netzwerken

Klassische OK übernimmt die Täter-Netzwerke

„Geschäftsausdehnung“ in allen Bereichen

DIE GEFAHR NIMMT TENDENZIELL ZU!

CAAS – GEGENMASSNAHMEN

INTEGRIERTES SICHERHEITSMANAGEMENT

- **Awareness**
- **Präventionsmaßnahmen, z.B.Honeypots**
- **Detektionsmaßnahmen, z.B. Anomalie-Programme**
- **...**

INFORMATIONS- UND ERFAHRUNGSAUSTAUSCH

- **mit Betroffenen (Opfer-Netzwerke)**
- **mit Sicherheits-Experten (Experten-Netzwerke)**
- **mit Sicherheitsbehörden (Modi Operandi, Maßnahmen der Strafverfolgung)**
- **...**

DISKUSSION

MAGENTA SECURITY

VIELEN DANK!

ERLEBEN, WAS VERBINDET.