



Polizei

Hamburg

LKA 54 Cybercrime

ZENTRALE ANSPRECHSTELLE CYBERCRIME
Aktuelle Phänomene und Handlungsempfehlungen



- Sönke Rasmussen
- Seit 2011 bei der Hamburger Polizei
- 2017 Wechsel zur Kriminalpolizei
- Bachelorarbeit zum Thema Kryptowährungen und Geldwäsche
- 2019-2024 Cybercrime-Ermittler
- Seit 2024 Zentrale Ansprechstelle Cybercrime des LKA HH
- Blockchain Ermittlungen
- Verhandlungsgruppe des LKA





Agenda – 20 Min

- Was ist die ZAC?
- „Cybercrime“ aktuell
- Welche Angriffe finden tatsächlich statt?
- Drei Irrtümer, die den Tätern in die Hände spielen
- Was tun im Ernstfall
- Was macht die Polizei und was macht sie nicht?
- Die wichtigsten Handlungsempfehlungen





Was ist die ZAC?

Zen
Wir

Erreichbarkeiten der Zentralen Ansprechstellen Cybercrime (NUR FÜR UNTERNEHMEN)

	Land/Bund	Telefonnummer	E-Mailadresse	Webseite
	Baden-Württemberg	+49 711 5401-2444		Zur Website ➔
	Bayern	+49 89 1212-3300		Zur Website ➔
	Berlin	+49 30 4664-972972	✉ zac@polizei.berlin.de	
	Brandenburg	+49 3334 388-8686	✉ zac@polizei.brandenburg.de	
	Bremen	+49 421 362-19820	✉ cybercrime@polizei.bremen.de	
	Hamburg	+49 40 4286-75455	✉ zac@polizei.hamburg.de	Zur Website ➔

Im Falle

Die Zen

Ihnen a

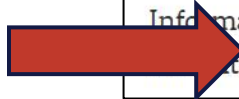
Info n

n für

haft stehen

l für

aten gegen





Was ist die ZAC?

- Die zentrale Ansprechstelle Cybercrime für die Hamburger Wirtschaft
- Beratungsangebote, präventive Awareness Schulungen und Incident Response Übungen
- Beratung in Ernstfällen
- Bindeglied zu den ermittlungsführenden Dienststellen in Hamburg und internationalen Fachdienststellen





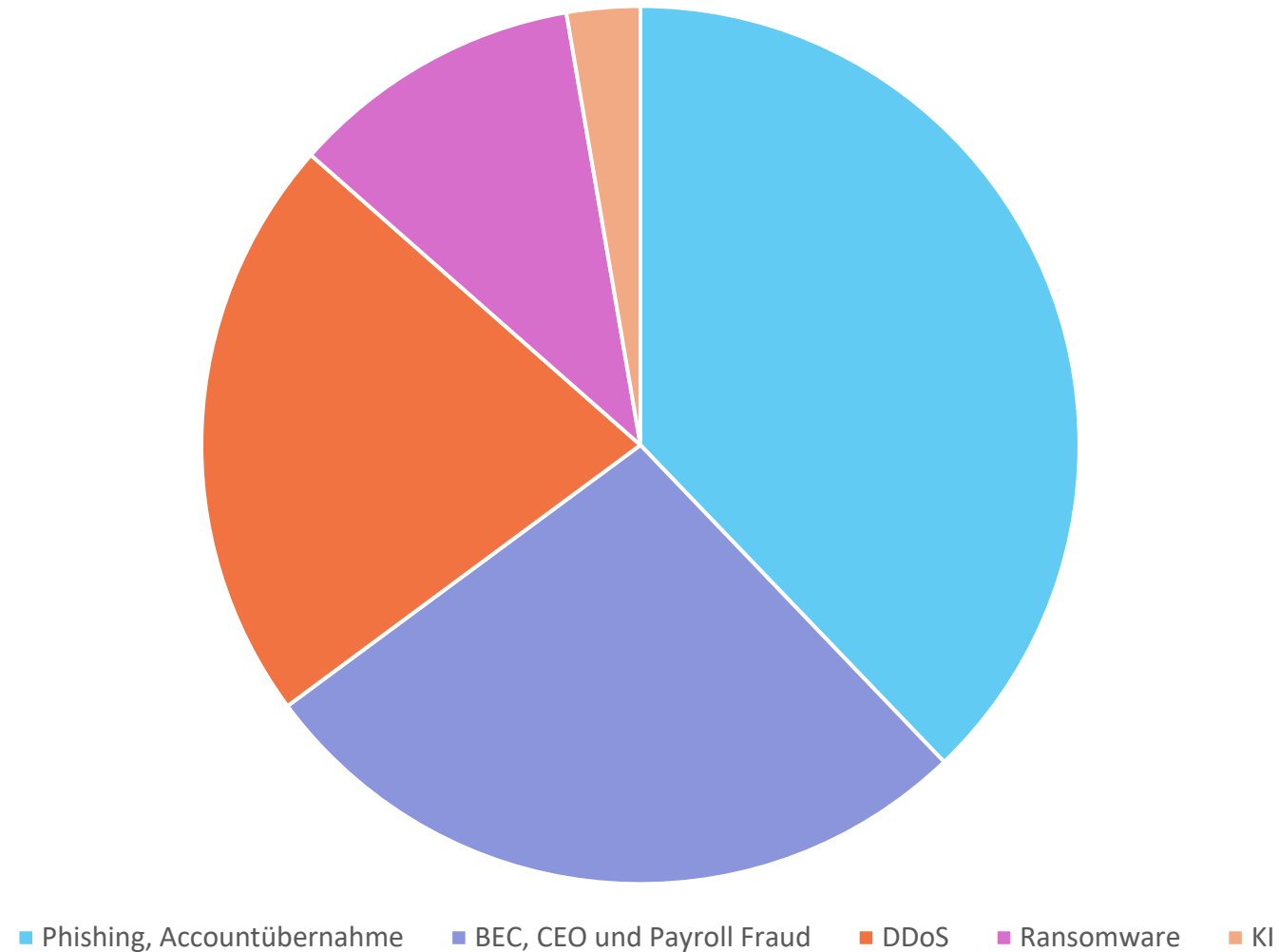
„Cybercrime“ aktuell

(aus polizeilicher Sicht)

- Vermehrtes Aufkommen und Ausnutzen sog. Zero-Day Schwachstellen
- Zuwachs politisch motivierter Cyberkriminalität
- Vibe-Coding und Verhandlungs-Bots bei Ransomware-Gruppierungen
- Insgesamt sehr wenige Fälle, bei denen KI eine entscheidende Rolle gespielt hat
- Hohes Dunkelfeld, da viele Scan- und Zugriffsaktivitäten nicht bemerkt oder zumindest nicht angezeigt werden



Welche Angriffe finden tatsächlich statt?





Drei Irrtümer, die den Tätern in die Hände spielen

1. *„Wir sind zu klein, um interessant zu sein / Wir haben keine wertvollen Daten.“*
2. *„Cyberbedrohungen wie Ransomware betreffen nur die IT.“*
3. *„Wir haben doch ein Backup.“*



Was tun im Ernstfall?

Ruhe bewahren und Überblick verschaffen	
IT / Cyberversicherung / externe Hilfe informieren	
Sofortmaßnahmen	Netzwerke trennen, Backups prüfen, alle aktiven Sessions beenden und VPN Zugänge sperren
ZAC informieren und telefonisch beraten lassen	040 4286 75455 zac@polizei.hamburg.de (bei akuten Notfällen auch 110 möglich)
Vorgehen dokumentieren	
Digitale Spuren sichern	
Weitere Stellen informieren	Datenschutzbehörde ggf. Hausbank, Kunden, Lieferanten etc.
Auf weitere Einschläge vorbereiten	z.B. Anfragen von Kunden und der Presse



Was macht die Polizei und was macht sie nicht?

- Awareness-Maßnahmen vor dem Ernstfall
 - Geschäftsleitung
 - Mitarbeitende
 - Incident Response Übung
 - Unterstützung während des Ernstfalls
 - Ermittlung der Täter
- Tatort absperren und alle Geräte beschlagnahmen
 - Systeme wieder aufsetzen
 - Geld sofort wiederbeschaffen
 - Ein individuelles Sicherheitskonzept für Ihr Unternehmen erstellen

CRIME SCENE - DO NOT CROSS

CRIME SCENE - DO NOT CROSS



Die wichtigsten Handlungsempfehlungen

- Setzen Sie sich frühzeitig (vor dem Ernstfall) mit dem Thema auseinander
- Verschaffen Sie sich einen Überblick über Ihren Daten und Systeme
- Suchen Sie ggf. jetzt schon Kontakt zu Unternehmen und Stellen, die Sie im Notfall unterstützen könnten
- Investieren Sie in Ihre IT-Sicherheit
- Machen Sie Ihre Backups krisensicher
- Schulen Sie Ihre Mitarbeitenden (fortlaufend)
- Steigern Sie Ihre Cybercrime-Resilienz mit kleinen Notfallübungen und verlassen Sie sich nicht auf Handbücher



Vielen Dank für Ihre Aufmerksamkeit



ZAC Kontakt