Cybercrime aus polizeilicher Sicht

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

Bedrohungslage und Phänomene

Silvio Berner, Kriminalkommissar

SN4C
CyberCrime
Competence
Center
Sachsen

Agenda

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

Wovon spricht die Polizei bei Cybercrime?

Phänomene,Trends, Lage

Was können Unternehmen tun?

SN4C CyberCrime Competence Center Sachsen

192.168

Control Status

SENSOR	ACTUAL	SETPOINT	STATUS
Cook	113 C	135 C	LOW
Food1	OPEN	0 C	ERROR
Food2	OPEN	0 C	ERROR
Food3	OPEN	0 C	ERROR
OUTPUT	100 %		
TIMER	00:00:00		

Submit Values | Cancel Changes | Reboot Device

BBQ GURU

CyberQ Temperature Controller

Main Screen | System Setup | Control Setup | WIFI Setup | Email Aler

Wovon spricht die Polizei bei Cybercrime?

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Wovon spricht die Polizei bei Cybercrime?

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Cybercrime im **engeren** Sinne – Straftaten **auf** IT
- Cybercrime im **weiteren** Sinne – Straftaten **mittels** IT
- Die Angreifer lassen sich in folgende Gruppen unterteilen:
  - Skript Kiddies
  - Cyber Kriminelle
  - Cyber Aktivisten
  - Staatlich unterstütze Organe (Nachrichtendienste etc.)

Rolle der Polizei

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Gefahrenabwehr und Strafverfolgung
  - Keine Datensicherung von Systemen
  - Keine Wiederherstellung
  - Keine sonstigen IT-Dienstleistungen

Zuständigkeit bei Cybercrime-Delikten

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Zuständigkeit ist Delikts-und Ortsabhängig
- Beratung und Unterstützung durch Zentrale Ansprechstelle Cybercrime
- Aufklärung und Spurensicherung

SN4C CyberCrime Competence Center Sachsen

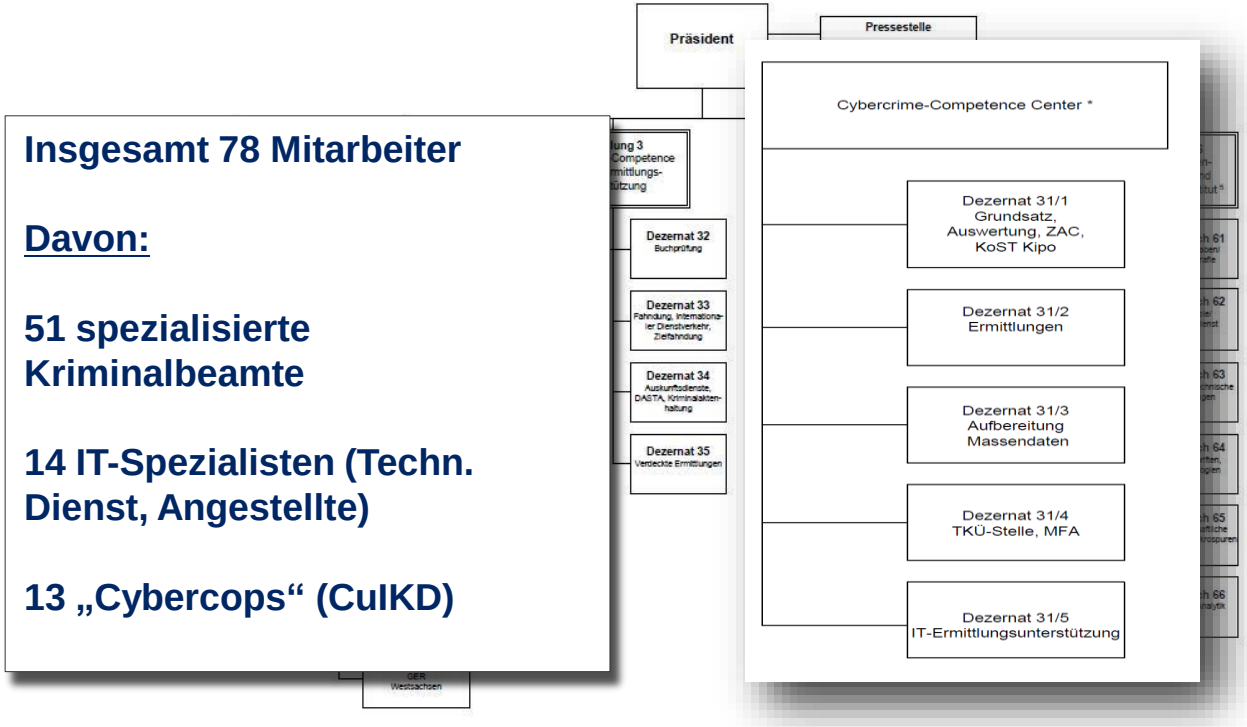
Insgesamt 78 Mitarbeiter

<u>Davon:</u>

51 spezialisierte Kriminalbeamte

14 IT-Spezialisten (Techn. Dienst, Angestellte)

13 „Cybercops“ (CuIKD)



Das Strafverfahren

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Cybercrime fast alles Antragsdelikte → Strafantrag (Antragsberechtigter?)
- Polizei ist die Ermittlungsbehörde der Staatsanwaltschaft
- Staatsanwaltschaft entscheidet über Strafbefehl, Anklageerhebung, Einstellung des Verfahrens oder weitere Ermittlungen

Aktuelle Phänomene

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

Großflächige Angriffe per Mail

Phishing und SPAM

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

- Das Ziel ist eine möglichst große Zahl von E-Mail-Postfächern und somit Opfern zu erreichen.
- Die Täter kennen die Opfer nicht = es kann jeden Treffen dessen E-Mail auf der Liste steht.
- Sie erhalten eine E-Mail die sie durch einen interessanten oder wichtigen Sachverhalt dazu bringen soll einem Link zu folgen oder einen E-Mail-Anhang zu öffnen.
- In diesem Augenblick laden sie sich die Schadsoftware auf ihr Smartphone oder Computer

Phishing
→ Gefährliche Umleitung für Ihre Passwörter…

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Das Wort setzt sich aus "Password" und "fishing" zusammen, zu Deutsch "nach Passwörtern angeln".
- Phishing-Betrüger fälschen z.B. **E-Mails** und **Internetseiten** und finden immer wieder neue Wege, um an vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern heran zu kommen – die Nutzer geben ihre Daten einfach freiwillig preis. (unbemerkt)
- Das „knacken“ von Passwörtern ist somit nicht erforderlich.

SN4C CyberCrime Competence Center Sachsen

CEO Fraud
(Business Email Compromise)

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

- Vortäuschung einer persönlichen Beziehung zum Opfer
  - Man-in-the-Middle-Attack
  - CEO-Fraud
  - Betrügerische Rechnung
  - Account Compromise (tatsächlicher Hack)
  - Datendiebstahl (Ziel: Personalabteilung)

SN4C CyberCrime Competence Center Sachsen

Identitätsdiebstahl (Identity Theft)

- Missbrauch des eigenen Namens oder persönlicher Daten durch unbefugte Dritte.
- **Mittels:**
  - Malware, Social Engineering, Eingabe von Daten vorgetäuschter Websites, Hacking
- **Ziele** sind Zugangsdaten zu Accounts jeglicher Art
  - E-Mail, Online-Banking, Online Shops, Firmenzugänge, Kreditkartendaten, Zahlungsdaten

Formen des Identitätsmissbrauchs im Internet

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- **Waren-Bestellungen**: In diesem Fall bestellt der Kriminelle unter dem Name und der Adresse des Opfers z.B. bei Online-Shops.
- **Erstellung falscher Profile in sozialen Netzwerken:** Hier erstellt der Täter in sozialen Netzwerken wie z.B. Facebook unter dem Namen seines Opfers.
- **Anmietung von Infrastruktur zur Tatbegehung**: z.B. Server, Paypal, Konten …
- **Versand von Spam im Namen des Opfers:** Ziel ist die Verteilung von gefälschten Rechnungen oder Schadsoftware

Digitale Erpressung mittels Ransomware

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- **Ransomware** (Lösegeld/Erpressung) + **Malware** (Schadsoftware)
- Vollverschlüsselung (auch Netzpartitionen und externer Speicher) oder Sperrung des Systems
- Vermeintliche Freischaltung gegen Bezahlung (meist Bitcoin)
- Vielfältige Angriffswege (meist Mails mit Links oder Anhängen, drive-by download, Serverschwachstellen, Fernwartungszugänge)
- Das Phänomen betrifft Privatpersonen wie auch Firmen. Im Falle einer Nicht-Zahlung wird ggf. mit der Veröffentlichung privater Daten bzw. Firmendaten gedroht.

Fake-Shops

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Kunden werden verschiedenste Produkte zu unschlagbar günstigen Preisen angeboten
- es wird die Zahlung mittels Vorauskasse, Voucher oder Western Union verlangt
- die versprochene Ware wird nicht geliefert oder nur in mangelhafter Qualität
- Ein Fake-Shop ist nie sehr lange online!
  (In der Regel wird die Website nach nur wenigen Tagen oder Wochen von den Betrüger/innen wieder offline genommen)

SN4C CyberCrime Competence Center Sachsen

Crime as a Service

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- im clear-web und im deep-web
- Verfügbarkeit aller für die Begehung von Straftaten notwendigen Anwendungen im Netz
- Illegale Marktplätze mit Kaufhaus-Charakter
- Zugang für alle Nutzer
- Keine Expertise erforderlich!
- Arbeitsteiliges Zusammenwirken verschiedener Akteure
- Serviceleistung für Kunden (Betreuung, Beratung)

Crime as a Service

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Zugangsdaten zu Online-Diensten, Kreditkartendaten
- Technische Dienstleistungen
- Hacking-Dienstleistungen und Hacking-Tools
- Malware
- Sicherheitsdienstleistungen
- Finanzdienstleistungen
- Logistikdienstleistungen

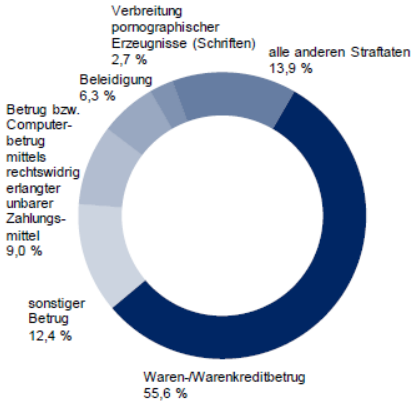
Aktuelle Zahlen

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

Entwicklung der Cybercrime (Hellfeld)

LANDES-KRIMINALAMT | POLIZEI Sachsen

- Bedrohungspotenzial durch Cybercrime steigt weiter
- Anstieg der Cybercrime im engeren Sinne (Angriffe auf Datennetze) um 23,7 Prozent (2017: 2.652 Fälle, 2016: 2.144 Fälle)
- Anstieg der Straftaten mit dem Tatmittel Internet um 8,8 Prozent (2017: 11.173 Fälle, 2016: 10.269 Fälle)



Anzahl erfasster Fälle Tatmittel Internet		
Straftatenobergruppe	Jahr 2016	Jahr 2017
Straftaten insgesamt	10.269	11.173
Waren-/Warenkreditbetrug	5.188	6.207
sonstiger Betrug	2.054	1.388
Betrug bzw. Computerbetrug mittels rechts-widrig erlangter unbarer Zahlungsmittel	469	1.011
Beleidigung	652	709
Verbreitung pornographischer Schriften (Erzeugnisse)	207	300
alle anderen Straftaten	1.699	1.558

SN4C CyberCrime Competence Center Sachsen

Entwicklung der Cybercrime (Dunkelfeld)

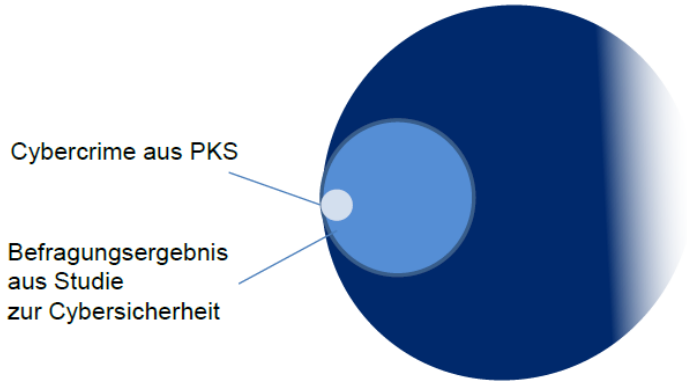
LANDES-
KRIMINALAMT

POLIZEI
Sachsen

- forsa-Studie im Auftrag des SMI zur Cybersicherheit in Sachsen
  - 1.000 Erwachsene befragt; davon nutzen 84 Prozent das Internet
  - 10 Prozent waren innerhalb der letzten zwölf Monate von einer Infizierung ihrer privaten Geräte durch Schadsoftware betroffen
  - 5 Prozent von Waren- und Dienstleistungsbetrug im Internet, 4 Prozent vom Diebstahl ihrer Identität sowie 1 Prozent von digitaler Erpressung
- Hochrechnung:
  - von den 840 Nutzern wurden 168 Cyberangriffe bemerkt
  - bei 2,92 Mio. Internetnutzern in Sachsen (84 Prozent von 3,47 Mio. Personen über 18 Jahre) entspräche das rd. 584.000 Sachverhalten

Entwicklung der Cybercrime (Hell-/Dunkelfeld, Ausblick)

LANDES-KRIMINALAMT | POLIZEI Sachsen



- **Was soll mit der Darstellung erreicht werden?**
  - Problembewusstsein vermitteln: jeder kann Opfer eines Cyberangriffs werden, Firmen, Privatpersonen, chattende Kinder und Jugendliche
  - Verdeutlichen: man kann sich gegen derartige Angriffe schützen; hier sind die Nutzer selbst, die Anbieter von Internetdiensten und der Staat gefordert
  - Handeln: Cybersicherheitsgesetz erarbeiten; Ausbau der polizeilichen Kompetenzen (SN4C); Ausbildung weiterer Informatiker zu „Cybercops“ (bisher 26 Absolventen)

Zusammenfassung

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Internetkriminalität hat das Potenzial zum Massendelikt ??? – ist ein Massendelikt!
- Alle Internetnutzer können weltweit von neuen kriminellen Erscheinungsformen sofort betroffen sein.
- Täter arbeiten schnell, weltweit, organisiert und flexibel.
- Nationale Grenzen spielen keine Rolle.
- Die Professionalisierung der Internet-Kriminellen hat unabhängig von der Entwicklung statistischer Daten zugenommen.
- Die modi operandi (Art des Handelns) werden ständig neu- bzw. weiterentwickelt.

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Wie können Sie Ihr Unternehmen schützen?

Präventive Maßnahmen - Awareness (Achtsamkeit)

LANDES-KRIMINALAMT | POLIZEI Sachsen

- Bewusstsein gegenüber der Gefahren durch Cybercrime
- Auseinandersetzung mit Sicherheitsvorfällen – Incident Response
- Verantwortung für die bei Ihnen gespeicherten Daten, auch Kundendaten
- Kosten für Schutzmaßnahmen < Kosten eines Cyber-Angriffs

Präventive Maßnahmen - Schutz für Unternehmen

LANDES-KRIMINALAMT | POLIZEI Sachsen

- Auseinandersetzung mit der Thematik:
  - Internetseite der Allianz für Cyber-Sicherheit (BSI)
  - Frei zugängliche Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime
  - Branchenverbände z.B. ASW, IHK, HWK, Bitkom etc.

Präventive Maßnahmen - Schutz für Unternehmen

LANDES-KRIMINALAMT | POLIZEI Sachsen

- Erstellen und Umsetzen eines IT-Sicherheitskonzeptes, welche u.a. Maßnahmen für folgende Bereiche festlegen sollte:
  - Technische IT-Sicherheit (z.B. Firewalls, Verschlüsselung, Netztrennung etc.)
  - Organisatorische Sicherheit (z.B. Richtlinien, Notfallpläne)
  - Physische Sicherheit (z.B. Gebäudeschutz, Überwachung)
  - Personelle Sicherheit (z.B. Schulungen, Sicherheitsüberprüfungen)
- Holen Sie professionelle Hilfe und Beratung!

Verhalten im Schadensfall

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Informationen sammeln, Beweise sichern. Identische Kopie des betroffenen Systems erstellen (Schaden abschätzen)
- alle damit zusammenhängenden Ereignisse (z.B. Anrufe, E-Mails, Systemstörungen, Logdaten) dokumentieren
- **Im Falle eines Cybercrime-Vorfalles ist ein entschlossenes und schnelles Handeln erforderlich!**
- Anzeige bei der Polizei erstatten (Online Anzeige)
- Meldung des Sachverhaltes bei der **Zentralen Ansprechstelle Cybercrime (ZAC) der Polizei – W-Fragen**

SN4C CyberCrime Competence Center Sachsen

Die Zentrale Ansprechstelle Cybercrime (ZAC)

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Die Zentrale Ansprechstelle Cybercrime

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

- **Ansprechpartner** zum Thema Cybercrime für Unternehmen, Verbände und Behörden des Freistaates Sachsen
- **Entgegennahme** von Sicherheitsvorfällen mit Bezug zu Cybercrime (telefonisch oder per E-Mail)
- **Beratung** zum weiteren Vorgehen nach Sicherheitsvorfällen mit Cybercrime Bezug
- **Förderung** der vertrauensvollen Zusammenarbeit zwischen Unternehmen, Verbänden, Behörden und der Polizei
- **Kontakt**: Montag bis Freitag von 08:00 bis 16:00 Uhr
- **Telefon**: 0351 855 3226 oder **E-Mail**: zac.lka@polizei.sachsen.de

SN4C CyberCrime Competence Center Sachsen

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Danke für Ihre Aufmerksamkeit!