POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

Herrenberg Digital XIII

Cybersecurity – ein falscher Klick

10.10.2023

KR Alexander Gehrig, M. eng.

Agenda

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

- Die Kriminalpolizeidirektion Böblingen / K5
- Phänomene und Präventionsmöglichkeiten
  - Phishing
  - Fake-Anrufe
  - Business Email Compromise (BEC)
  - Ransomware
- Fazit
- Erreichbarkeiten

Phishing

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

„Früher“

- Schlecht gemachte Spam-Emails
  - Rechtschreibung
  - Grammatik
  - fehlende / falsche Anrede
- „mit der Gießkanne“

„Heute“

- gezielter Versand von Spam-Emails
  - bessere sprachliche Qualität
  - häufig korrekte Anrede
- Daten stammen aus
  - Leaks
  - Stellenausschreibungen
  - sozialen Netzwerken
  - exfiltrierten Daten

Präventionsmöglichkeiten

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

- Email-Adresse des Absenders überprüfen
- Motivation des Nachrichtenversands hinterfragen
- Prüfung des Nachrichteninhalts
- Links nicht anklicken
- bei Aufforderung zur Eingabe von Zugangsdaten skeptisch sein
- im Zweifel nichts tun und Email dem (angeblichen) Absender sowie dem IT-Ansprechpartner melden
- Schulung der Mitarbeiter

Fake-Anrufe

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

- Anrufe von…
  - Microsoft
  - PayPal
  - etc.

- Hotline will per Fernwartung angebliche Probleme / Hackerangriffe beseitigen
- dabei werden freundlicherweise auch die Bankkonten / Kreditkarten mit einbezogen

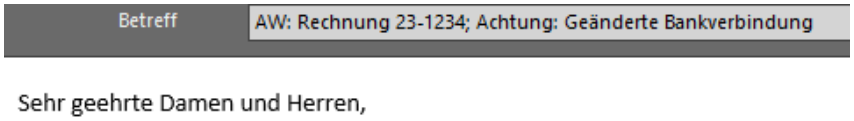
Präventionsmöglichkeiten

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

- keinen Fernzugriff gewähren
- keine Zugangsdaten weitergeben oder selbst eingeben
- am besten einfach auflegen

Business Email Compromise

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG



- verschiedene Ausprägungsformen
  - CEO-Fraud
  - Man in the Middle-Angriffe (geänderte Rechnung mit neuer Bankverbindung)
- in der Regel im Zusammenhang mit größeren Zahlungen
- Einfallsvektor derzeit Phishing und schwach abgesicherte Email-Postfächer (Outlook Web Access)
- Abfangen und Mitlesen der legitimen Emails
- täterseitige Nutzung eigens dafür angelegter Domains

Präventionsmöglichkeiten

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

- Etablierung eines Prozesses bei Veränderungen der Bankverbindung
  - immer gegenprüfen
  - Nachfragen auf einem separaten Kommunikationskanal
- Einsatz digitaler Signaturen
- Zwei-Faktor-Authentifizierung für Outlook Web Access
- regelmäßige Überprüfung der eingesetzten Systeme
  - ungewöhnliche Email-Konten
  - Regeln zum Löschen oder Weiterleiten von Emails
- Schulung der Mitarbeiter

Ransomware

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

„Früher“

- ungezielte Angriffe
- eher geringe Geldforderungen
- Infektion über Email-Anhänge
- Privatpersonen und Unternehmen

„Heute“

- gezielte Angriffe
- hohe und individuelle Geldforderungen
- Ausnutzen von Schwachstellen bzw. Fernzugriffsmöglichkeiten
- fast ausschließlich Unternehmen

State of the Art bei Ransomware

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

- zunehmende Professionalisierung (RaaS) mit Aufgabenteilung
- Opfer werden zuvor ausgekundschaftet
  - Angriffsvektoren
  - Wirtschaftsleistung
  - Kosten- / Nutzenabwägung der Täter
- gezieltes Ausnutzen von Schwachstellen, auch bereits kurz nach deren Bekanntwerden
- Double Extortion

Präventionsmöglichkeiten #1

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

- Offline-Backups
- Systeme aktuell halten (Patch Management)
- Angriffsfläche reduzieren
  - nur unbedingt erforderliche Fernzugriffsmöglichkeiten mit hoher Absicherung (MFA)
  - nur benötigte Software einsetzen
- Monitoring der Systeme (Firewall, IDS/ IPS)
- regelmäßig auf Anzeichen einer Kompromittierung prüfen (IoC)

Präventionsmöglichkeiten #2

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

- Netze trennen
- restriktive Rechtevergabe (least privileges)
- Admin-Zugänge nur mit MFA zulassen
- Krisenplan erstellen und testen
- Schulung der Mitarbeiter

Fazit

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

- Risiken können verringert werden
- eine Absicherung zu 100 % ist nicht möglich
- Mitarbeiter als essentieller Bestandteil der Sicherheit

Erreichbarkeiten

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM LUDWIGSBURG

- K5 der KPDir Böblingen zu üblichen Bürozeiten unter

  07031 13-1500

- Zentrale Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt Baden-Württemberg unter

  0711 5401-2444

  cybercrime@polizei.bwl.de

- Online-Wache unter

  https://www.polizei-bw.de