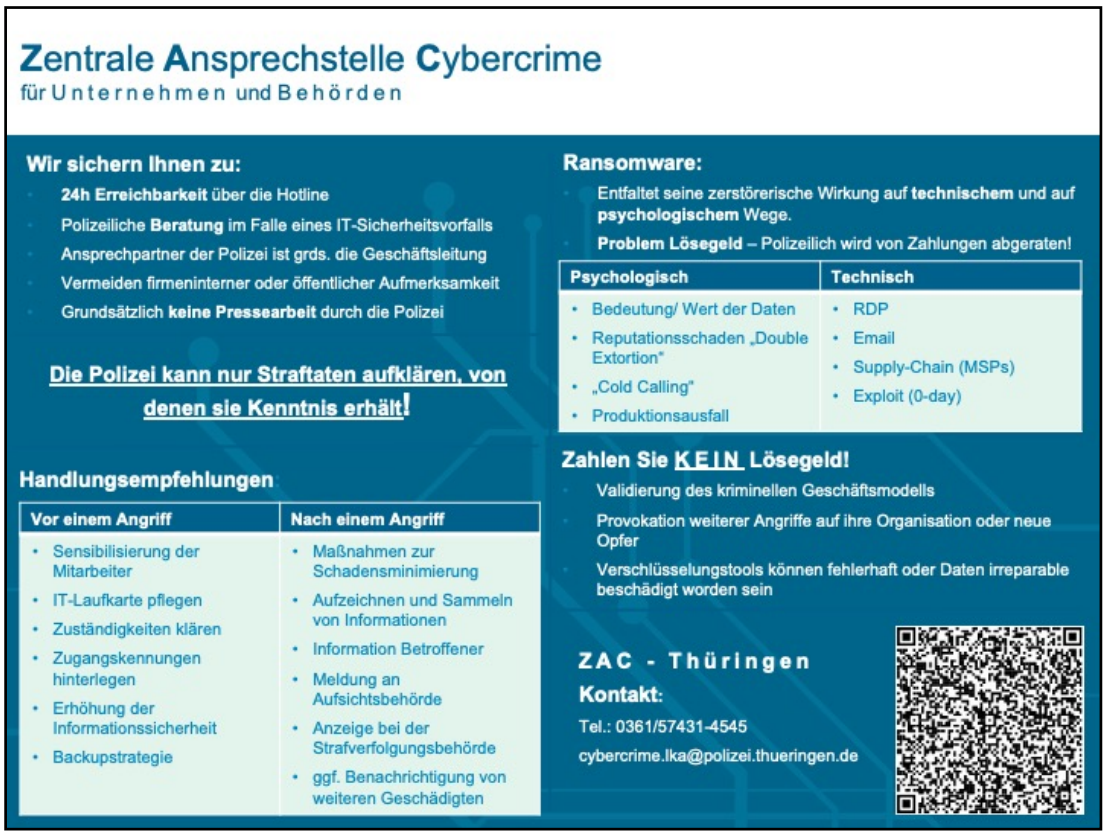

Die Folgenden präventiven Informationen sind lediglich exemplarisch, nicht abschließend und basieren auf polizeilichem Erfahrungswissen. Sie haben keinen Anspruch auf Vollständigkeit und entfalten keine Schutzgarantie im Falle Cyber-Angriffen!

Hinweise für den Anzeigenerstatter

- Meldeverpflichtung ggü. der Aufsichtsbehörde gemäß Art. 33 DSGVO - nur nötig bei Verletzung des Schutzes personenbezogener Daten
- grundsätzlich unverzüglich
- spätestens 72 Stunden nach Feststellung
- Infizierte Systeme nicht zur Kommunikation nutzen
- Information der Geschäftspartner und der Mitarbeiter über Sicherheitsvorfall - bei Verdacht das es sich um einen Innentäter handelt nach dem Prinzip handeln: "Kenntnis nur wenn nötig"
- Warnung der Geschäftspartner über eventuellen unberechtigten Versand von Mails im Namen der Firma, ggf. mit Rechnungsanhang
- vorherige Information der ZAC bei geplanter Kontaktaufnahme mit dem Erpresser (Einschaltung der Verhandlungsgruppe prüfen)
- Pressearbeit erfolgt nicht durch die Polizei (max. Hinweis auf laufende Ermittlungen), Abstimmung zum Wording ggü. der Presse im Unternehmen erforderlich

Quickcheck:

- Logfiles sichern (Analyse)
- Betroffene Systeme/Dateien ermitteln
- Betroffene Systeme aus Operationen herausnehmen und mit Backups ersetzen
- Andere Systeme prüfen
- Betroffene Systeme wiederherstellen und updaten
- Daten- und andere Verluste analysieren
- Problem melden!

IT-Laufkarte – Beispiel:

- Netzplan/Netzstruktur
- Angaben zur Serverstruktur (Standort/Vernetzung)
- **Erreichbarkeiten (Admin, IT-Dienstleiter, Versicherung)**
- Kenntnis der Zugangsdaten (auch für Cloud-Dienste)
- Internetanschlüssen innerhalb des Unternehmens
- Weitere Netzwerkzugänge innerhalb des Unternehmens

Backup

3-2-1 Methode

- 3 Kopien auf
- 2 verschiedenen Medien und
- 1 Georedundanz (Feuerfest)

WCIHTIG: Test auf Funktionsfähigkeit

Lösegeld???

- Validierung des Geschäftsmodells
- Provokation von Angriffen z. N. andere Opfer
- Provokation von neuen Angriffen z. N. des eigenen Unternehmens
- Ransomware-Gruppierungen können sog. „0-day"-Schwachstellen testen und Exploits weiterentwickeln
- **Entschlüsselung?**
    1. Daten können während des Verschlüsselungsprozesses irreparabel beschädigt werden
    2. Entschlüsselungstool kann mit weitere Malware kommen, funktioniert nicht oder nur sehr langsam
    3. Überlastung des Täters (fehlerhafte Entschlüsselungstools, falsche Opfer-IDs)

Was braucht der Ermittler? [nicht abschließend]

- Angriffsmail
- 2 Beispieldateien < 1 MB
- das Erpresserschreiben
- Bitcoin-Adresse(n)
- Mail-Adressen des Täters
- Logprotokolle der relevanten Systeme sichern
- Eventlogs vom Server
- Eventlogs vom Client „Null“
- Extraktion (csv-File geplanter Tasks/ Prozesse betroffener Clients und Server
- Screenshot des „Autostart“ vom Client Null
- Malware-Sample zu Analysezwecken

Hinweise für den Anzeigenerstatter

- Meldeverpflichtung ggü. der Aufsichtsbehörde gemäß Art. 33 DSGVO - nur nötig bei Verletzung des Schutzes personenbezogener Daten
    - grundsätzlich unverzüglich
    - spätestens 72 Stunden nach Feststellung
- Infizierte Systeme nicht zur Kommunikation nutzen
- Information der Geschäftspartner und der Mitarbeiter über Sicherheitsvorfall - bei Verdacht das es sich um einen Innentäter handelt nach dem Prinzip handeln: "Kenntnis nur wenn nötig"
- Warnung der Geschäftspartner über eventuellen unberechtigten Versand von Mails im Namen der Firma, ggf. mit Rechnungsanhang
- vorherige Information der ZAC bei geplanter Kontaktaufnahme mit dem Erpresser (Einschaltung der Verhandlungsgruppe prüfen)
- Pressearbeit erfolgt nicht durch die Polizei (max. Hinweis auf laufende Ermittlungen), Abstimmung zum Wording ggü. der Presse im Unternehmen erforderlich