LHL

DIGITALISIERUNG. AUTOMATISIERUNG. EDV.

IT-Sicherheit im Jahr 2024:

Die aktuelle Bedrohungslage

DATEV CORPORATE PARTNER

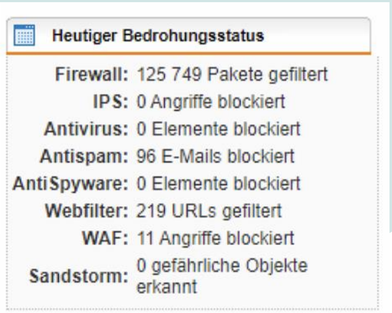
DATEV SOLUTION PARTNER

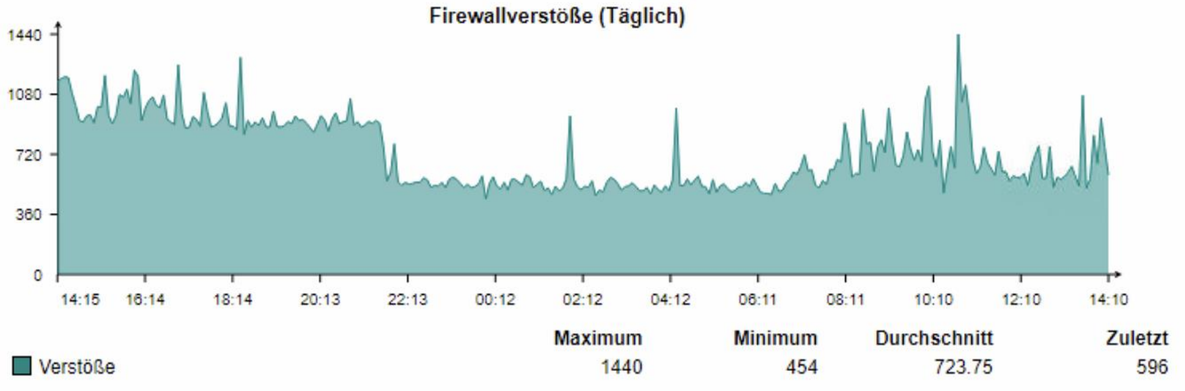
DATEV DMS
Experte DATEV Unternehmen online
PARTNERasp

die system partner

Was passiert da draußen?

- „Auf unseren Firewalls tobt ein Krieg“
- Extrem hohe Anzahl erfolgreicher Attacken auf Unternehmen in Deutschland:
- Im Jahr 2022 wurden 139.000 Unternehmen in Deutschland gehackt – Dunkelziffer allerdings geschätzt 90% (Quelle: BKA)
- Laut Google 398 Millionen DDoS-Angriffe pro .....?
- Laut Bitkom waren 70% der deutschen Unternehmen nachweislich von Cyberangriffen betroffen
- Live: https://www.sicherheitstacho.eu/start/main

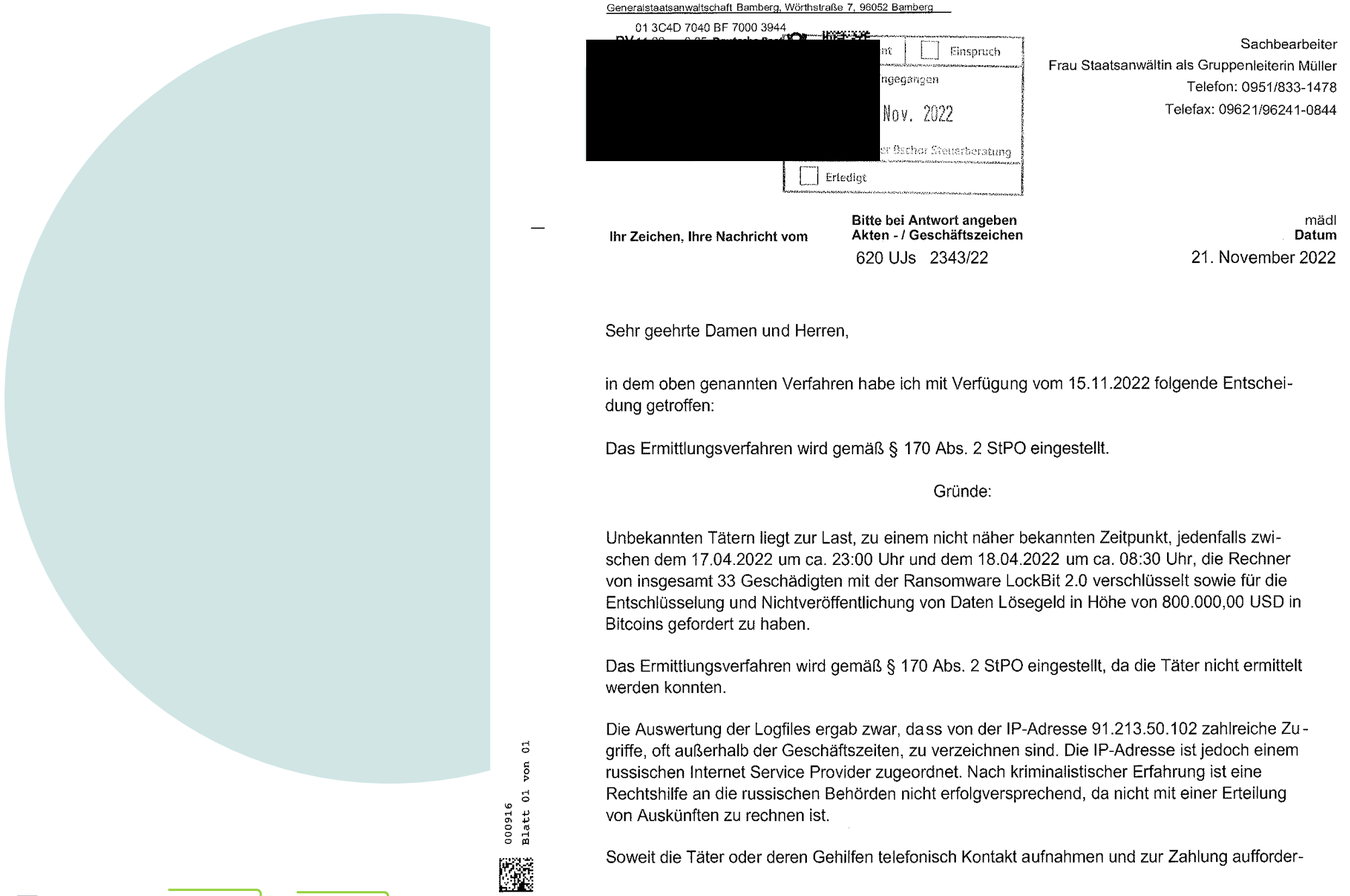




Was hat sich verändert – für StB´s?

– Extrem hohe Qualität der Angriffe
– Hacker haben einen sehr langen Atem, denn:
  • Angriffe laufen automatisiert („das Opfer sucht sich den Hacker“)
  • „Wer interessiert sich schon für meine kleine Steuerkanzlei?“
– Erpressung mit verschlüsselten Systemen und geklauten Daten ist ein Milliarden-$-Geschäft
– Kanzleien zahlen sehr gerne Lösegeld, warum wohl?
– Beispiele:
  • Gezielter Angriff auf Freiberufler: https://www.zdnet.de/88380873/ransomware-hakbit-greift-deutsche-user-an/
  • Angriff auf Kanzlei: https://www.kapellmann.de/de/nachrichten/kapellmann-opfer-eines-ransomware-angriffs

Was bedeutet ein Hack für eine Kanzlei?



Generalstaatsanwaltschaft Bamberg
Zentralstelle Cybercrime Bayern

Generalstaatsanwaltschaft Bamberg, Wörthstraße 7, 96052 Bamberg

01 3C4D 7040 BF 7000 3944

[redacted]

Einspruch

ngegangen

Nov. 2022

er Fischer Steuerberatung

Erledigt

Sachbearbeiter
Frau Staatsanwältin als Gruppenleiterin Müller
Telefon: 0951/833-1478
Telefax: 09621/96241-0844

Ihr Zeichen, Ihre Nachricht vom	Bitte bei Antwort angeben Akten - / Geschäftszeichen	mädl Datum
	620 UJs 2343/22	21. November 2022

Sehr geehrte Damen und Herren,

in dem oben genannten Verfahren habe ich mit Verfügung vom 15.11.2022 folgende Entscheidung getroffen:

Das Ermittlungsverfahren wird gemäß § 170 Abs. 2 StPO eingestellt.

Gründe:

Unbekannten Tätern liegt zur Last, zu einem nicht näher bekannten Zeitpunkt, jedenfalls zwischen dem 17.04.2022 um ca. 23:00 Uhr und dem 18.04.2022 um ca. 08:30 Uhr, die Rechner von insgesamt 33 Geschädigten mit der Ransomware LockBit 2.0 verschlüsselt sowie für die Entschlüsselung und Nichtveröffentlichung von Daten Lösegeld in Höhe von 800.000,00 USD in Bitcoins gefordert zu haben.

Das Ermittlungsverfahren wird gemäß § 170 Abs. 2 StPO eingestellt, da die Täter nicht ermittelt werden konnten.

Die Auswertung der Logfiles ergab zwar, dass von der IP-Adresse 91.213.50.102 zahlreiche Zugriffe, oft außerhalb der Geschäftszeiten, zu verzeichnen sind. Die IP-Adresse ist jedoch einem russischen Internet Service Provider zugeordnet. Nach kriminalistischer Erfahrung ist eine Rechtshilfe an die russischen Behörden nicht erfolgversprechend, da nicht mit einer Erteilung von Auskünften zu rechnen ist.

Soweit die Täter oder deren Gehilfen telefonisch Kontakt aufnahmen und zur Zahlung aufforder-

000916 Blatt 01 von 01

Datenschutzhinweis:
Informationen zum Datenschutz finden Sie unter www.justiz.bayern.de/gerichte-und-behoerden/generalstaatsanwaltschaft/bamberg/

Hausanschrift	Haltestelle	Geschäftszeiten	Kommunikation
Wörthstraße 7 96052 Bamberg	Weißenburgstraße Buslinie 901	Mo.-Fr. 08.00 - 12.00 Uhr, Mo. - Do. 13.00 - 15.00 Uhr	**Telefon:** 0951/833-0 **Telefax:** 09621/96241-0508 poststelle@gensta-ba.bayern.de

Die E-Mail-Adresse eröffnet keinen Zugang für formbedürftige Erklärungen in Rechtssachen

LHL
DIGITALISIERUNG. AUTOMATISIERUNG. EDV.

DATEV CORPORATE PARTNER

DATEV SOLUTION PARTNER

DATEV DMS
Experte DATEV Un
PARTNERasp

die system partner

LHL

DIGITALISIERUNG. AUTOMATISIERUNG. EDV.

IT-Sicherheit

Wie können wir dem Hacker das Leben schwer machen?

Wie können wir uns schützen?

- Normale Virenscanner sind fast nutzlos, notwendig sind moderne EDR/XDR-Systeme
  - KI-gestütztes Erkennen von Bedrohungen
  - Zusammenarbeit von UTM-Router, Virenscanner und Onlinequellen
  - Anti-Verschlüsselungstechniken auch bei unbekannten Schädlingen
  - Schutz vor Identitätsklau (Zugangsdaten, Passwörter)
- Moderne UTM-Firewalls
  - KI-gestützte Analysen des Datenverkehrs
  - E-Mail-Verkehr absichern
  - Links zur Aufrufzeit kontrollieren
- Der Client im Fokus:
  - EDR/XDR-Virenscanner
  - Patchmanagement: Zeitnahe Installation von Sicherheitsupdates
  - Begrenzung von Zugriffsmöglichkeiten, z.B. Sperren von USB-Ports (der Feind sitzt manchmal in der Kanzlei

Wie können wir uns schützen?

- 2-Faktor-Authentifizierung nutzen
  - Keine Klartextdateien im Dateisystem (Word, Excel, PDF):
    - Diese werden bevorzugt geklaut, da gut verwertbar
    - Ablage von Dokumenten in den DATEV-Produkten wie DMS oder Dokumentenablage
  - Nutzung von sicheren Produkten: DUO, ANO, Digitale Personalakte
  - Ländersperren setzen
  - Rechtestrukturen immer wieder überprüfen

ANGRIFFSPUNKT MENSCH

- Social hacking: https://www.golem.de/news/40-millionen-euro-gestohlen-wie-der-leoni-betrug-abgelaufen-ist-1609-123108.html
- Der USB-Stick im Treppenhaus.....
- Welche Informationen geben wir Preis?
- Wie können wir dem Menschen technisch unterstützen?:
  - Technische Möglichkeiten nutzen (Sperren, USB-Ports, EDR)
    - Zwei-Faktor-Authentifizierungen nutzen
    - Vier-Augen-Prinzip z.B. beim Überweisen (höherer Summen)
- Schulen, sensibilisieren
  - Erkennen verschlüsselter bzw. verdächtiger Websites
  - Wem gebe ich welche Zugangsdaten oder Informationen?
  - Im Idealfall: Fortlaufendes Training mit laufender Erfolgskontrolle

VORBEREITUNG AUF DEN FALL DER FÄLLE

- Backup ist notwendig
  - Zitat ct 24/2022: „kein Backup – kein Mitleid“
  - Mehrfache Backups, auch außerhalb der Reichweite von Hackern
  - Rücksicherungstests regelmäßig durchführen
  - Backup auf S3-Speicher ideal, seit Dezember 2023 im LHLasp verfügbar + Verfügbarkeit für On-Prem-System
- Anfertigung eines Notfallplans, nicht nur für IT!
- Abschluß bzw. Überprüfung einer Cyberversicherung
  - Absicherung des finanziellen Schadens
  - Hilfestellung bei der Kommunikation mit Kunden, Behörden, Öffentlichkeit und dem Hacker
  - Technische Hilfe vom Versicherer oder durch diesen organisiert

NEUE WEGE: LHLalarmanlage

- Die Lehre aus erfolgreichen Angriffen:
  - Hacker tümmeln sich lange und unerkannt in gehackten Netzwerken
  - Sammeln Informationen, Passwörter usw.
  - Infizieren immer mehr Systeme inkl. der lokalen Datensicherung
- Unsere Aufgabe: Entdecken dieser Aktivitäten
- Die Lösung: Ein Honigtopf
  - Ein passives System, das sich nicht wehrt
  - Sondern nur lauscht, auf typische Aktivitäten von Hackern
  - Alarmierung bei LHL (auf Wunsch auch beim Kunden)
- Frühere Entdeckung des Hackers, Verminderung des Schadens
- Februar 2023: Entdeckung eines Hacks in einer Steuerkanzlei

NEUE WEGE:
S3- / Immutable Backups

- Können wir verhindern, dass ein Hacker die Backups löscht oder manipuliert?:
- Ja, wir können in beiden Welten!
  - In LHLasp: Nutzung des S3-Speichers im DATEV-RZ
  - Bei Kunden mit EDV vor Ort: Nutzung S3-Speicher in der Cloud
- Früher war 3-2-1:
  - 3 Backups
  - 2 verschiedene Medien
  - 1 Kopie außerhalb der Kanzlei
- Jetzt ist 3-2-1-1-0
  - 1 Backup ist unveränderlich
  - 0 Fehler bei der Wiederherstellung

LHL
DIGITALISIERUNG. AUTOMATISIERUNG. EDV.

DATEV CORPORATE PARTNER
DATEV SOLUTION PARTNER
DATEV DMS
Experte DATEV Unternehmen online
PARTNERasp

die system partner