ATB. LAW

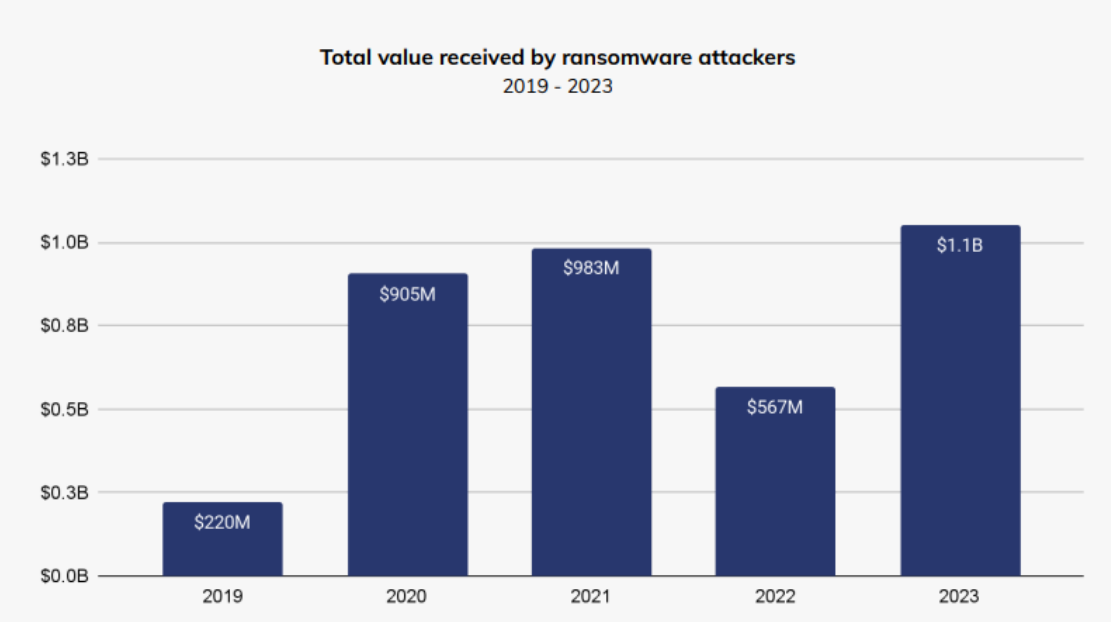
RANSOMWARE ANGRIFFE: Rechtliche Aspekte

Mag. Roman Taudes, LL.M.

ATB. LAW

RANSOMWARE-ANGRIFF

- WAS IST DAS?
  - Angriff auf ein Computersystem mit einer Schadsoftware
  - um Daten des Opfers zu verschlüsseln und/oder zu entwenden
  - damit Lösegeld gefordert
  - oder Daten verkauft werden können
- WER SIND DIE ANGREIFER
  - Kriminelle Organisationen
  - „Ransomware-as-a-Service“
- WER SIND DIE OPFER
  - (auch kleine) Unternehmen
  - Privatpersonen



Quelle: Chainalysis Crypto Crime Report 2024

ATB. LAW

RELEVANZ

IT-SICHERHEIT

Hackerangriff auf Kärnten: Erbeutete Date… wurden offenbar verkauft

Die Landesregierung verweigerte, das geforderte Lösegeld zu bezahlen. Nun Hackergruppe "Black Cat" die kopierten Daten offenbar weiterverkauft

3. Juli 2022, 12:48

SCHLECHTE WARTUNG

Neue Ransomware-Welle übernimmt weltweit tausende Server

Italienische Cybersicherheitsbehörde ACN warnt vor zahlreichen Attacken gegen eine Lücke in VMware ESXi. Für diese gibt es seit Februar 2021 Updates

6. Februar 2023, 13:30, 33 Postings

Hackerattacke

Datenleck bei Motel One betrifft Millionen von Kunden

Ende September machte die Hotelkette Motel One öffentlich, Ziel eines Ransomware-Angriffs geworden zu sein. Nun zeigen Recherchen der »Süddeutschen Zeitung« das Ausmaß des Angriffs – auch der Firmengründer ist betroffen.

…9.11 Uhr

westbahn.at

WESTbahn: Cybervorfall in den IT-Systemen - Fahrbetrieb nicht betroffen

Wien (OTS)- Im Laufe des Donnerstags, 19.10.2023 kam es zu einem Cybervorfall in den IT-Systemen der WESTbahn. Dieser Vorfall betrifft vor allem Systeme in der Verwaltung des Unternehmens.

CHRONIK

Hackerangriff auf WIFI Niederösterreich

Das Wirtschaftsförderungsinstitut (WIFI) Niederösterreich ist Opfer eines Hackerangriffs geworden. Kunden- und Trainerdaten seien nicht entwendet worden, heißt es. Verantwortlich könnte eine international agierende Hackergruppe sein.

6. Februar 2024, 16.42 Uhr

Teilen

Deloitte.

Deloitte Cyber Security Report: Die Hälfte der heimischen Unternehmen war schon Ransomware-Angriffen ausgesetzt

Jedes achte Unternehmen erlebt mittlerweile fast täglich eine Cyber-Attacke

Wien (OTS)- In den letzten zehn Jahren hat die Anzahl an Ransomware-Attacken in Österreich stark zugenommen. Eine neue repräsentative Studie von Deloitte und SORA belegt: Beinahe die Hälfte der befragten Unternehmen hat bereits selbst eine Ransomware-Attacke erlebt, 12 % werden sogar fast täglich angegriffen. Trotz dieser Bedrohungslage verfügen nur die wenigsten Betriebe über einen Krisen- oder Notfallplan für Cyber-Attacken.

Quellen: derStandard; Orf.at, OTS, Spiegel

ATB. LAW

RANSOMWARE-ANGRIFFE SIND STRAFBAR

- § 118a StGB – Widerrechtlicher Zugriff auf ein Computersystem
- § 119 StGB – Verletzung des Telekommunikationsgeheimnisses
- § 119a StGB – Missbräuchliches Abfangen von Daten
- § 126a StGB – Datenbeschädigung
- § 126b StGB – Störung der Funktionsfähigkeit eines Computersystems
- § 144 f StGB – Erpressung

ATB. LAW

MELDEPFLICHTEN DES OPFERS IM ANLASSFALL

ATB. LAW

MELDEPFLICHTEN

VERSICHERUNG

- Obliegenheit
- Notfallnummer
- Incident Response Team

ATB. LAW

MELDEPFLICHTEN

DATENSCHUTZ

- Ransomwareangriff = Databreach
  - Meldung an Datenschutzbehörde (Art 33 DSGVO)?
    - Unverzüglich - binnen 72 Stunden
  - Meldung an Betroffene Personen (Art 34 DSGVO)?
    - Unverzüglich
  - Dokumentationspflicht!

ATB. LAW

WIE MAN´S NICHT MACHT

„liebe Datenschutz Behörde,

Danke für die mail

wir haben und werden unsere gäste davon nicht informieren da wir unsere gäste nicht unnötig mit solchen kranken Vorfällen belasten werden... wir sind ein Bewusstseins und verströmen ausschließlich pure liebe [Anmerkung Bearbeiter/in: Sonderzeichen Herzerl und Sternderl aus Gründen der Darstellbarkeit entfernt.] und gute Laune

da wir wissen das Gedanken und Taten Materie erschaffen wird nichts schlimmes passieren. Wir wissen nämlich das es so sein wird!!!

*wir haben mit der Firma k*** security selbstverständlich Vorkehrungen getroffen um so etwas zukünftig zu unterbunden.*

wir haben diese Meldung nur gemacht damit unsere Versicherung zufrieden ist und wir den Schaden erstatten bekommen

*ich bitte euch diesen Vorfall mit diesem Email ruhen zu lassen und bin für weitere Fragen sehr gerne telefonisch erreichbar 0043***3*5*7*4*

mit herzlichen [Anmerkung Bearbeiter/in: Sonderzeichen Herzerl aus Gründen der Darstellbarkeit entfernt.]

*Grüßen aus dem B****

*Sebastian W****

*www.b***.at"*

DSB 12.12.2023, 0/1000

ATB. LAW

MELDEPFLICHTEN

GESCHÄFTSPARTNER

- Auftragsverarbeiter -> Verantwortlichen
- Daten des Geschäftspartners betroffen

ATB. LAW

MELDEPFLICHTEN

POLIZEI

- Keine gesetzliche Pflicht
- Allfällige indirekte Anzeigepflicht der GF
- Sinnvoll?

RANSOMWARE-ANGRIFFE

22.05.2024, 15:19 Uhr

Polizei warnt vor Hackerangriffen über Office-365-Komponenten

Immer mehr Unternehmen sind aktuell von Hackerangriffen auf Office 365 betroffen, wie jetzt das Landeskriminalamt NRW warnt. Vor allem die Funktionen E-Mail und Dokumentenverwaltung sind ins Visier von Kriminellen geraten.

OPERATION CRONOS

Internationale Ermittler enttarnen Kopf hinter der Erpresserbande Lockbit

Russe soll 100 Millionen Dollar mit Ransomware verdient haben. Polizei veröffentlicht Tool für die Opfer, damit sie ihre Daten entschlüsseln können

8. Mai 2024, 13:11, 53 Postings

ATB. LAW

MELDEPFLICHTEN

POLIZEI

- Verpflichtung aus Versicherungsvertrag

c. Obliegenheiten

Bei einer **Datenerpressung** sind die **Versicherten** zusätzlich zu den allgemeinen Obliegenheiten gemäß II Ziff. 3. dieses Vertrages verpflichtet:

- Der Versicherungsnehmer, seine Vertrauenspersonen und der Versicherer sind im Schadenfall verpflichtet, die Tat bei der Polizei unverzüglich anzuzeigen um das staatliche Strafverfolgungsinteresse zu unterstützen.

3.6. Rechtsfolgen einer Obliegenheitsverletzung

Im Falle der Verletzung einer Obliegenheit nach Eintritt des Versicherungsfalles ist der Versicherer von seiner Leistung frei. Dies gilt nicht, wenn die Verletzung weder auf Vorsatz noch auf grober Fahrlässigkeit beruht. Der vollständige oder teilweise Wegfall des Versicherungsschutzes hat bei Verletzung einer nach Eintritt des Versicherungsfalls bestehenden Auskunfts- oder Aufklärungsobliegenheit zur Voraussetzung, dass der Versicherer die jeweilige **Versicherte** durch gesonderte Mitteilung in Textform auf diese Rechtsfolge hingewiesen hat.

ATB. LAW

MELDEPFLICHTEN

SONSTIGE

- NISG – Netz- und Informationssystemsicherheitsgesetz
- Ad-hoc-Publizitätspflichten
- Meldepflichten an Aufsichtsbehörden
- u.A.

DOKUMENTATION !

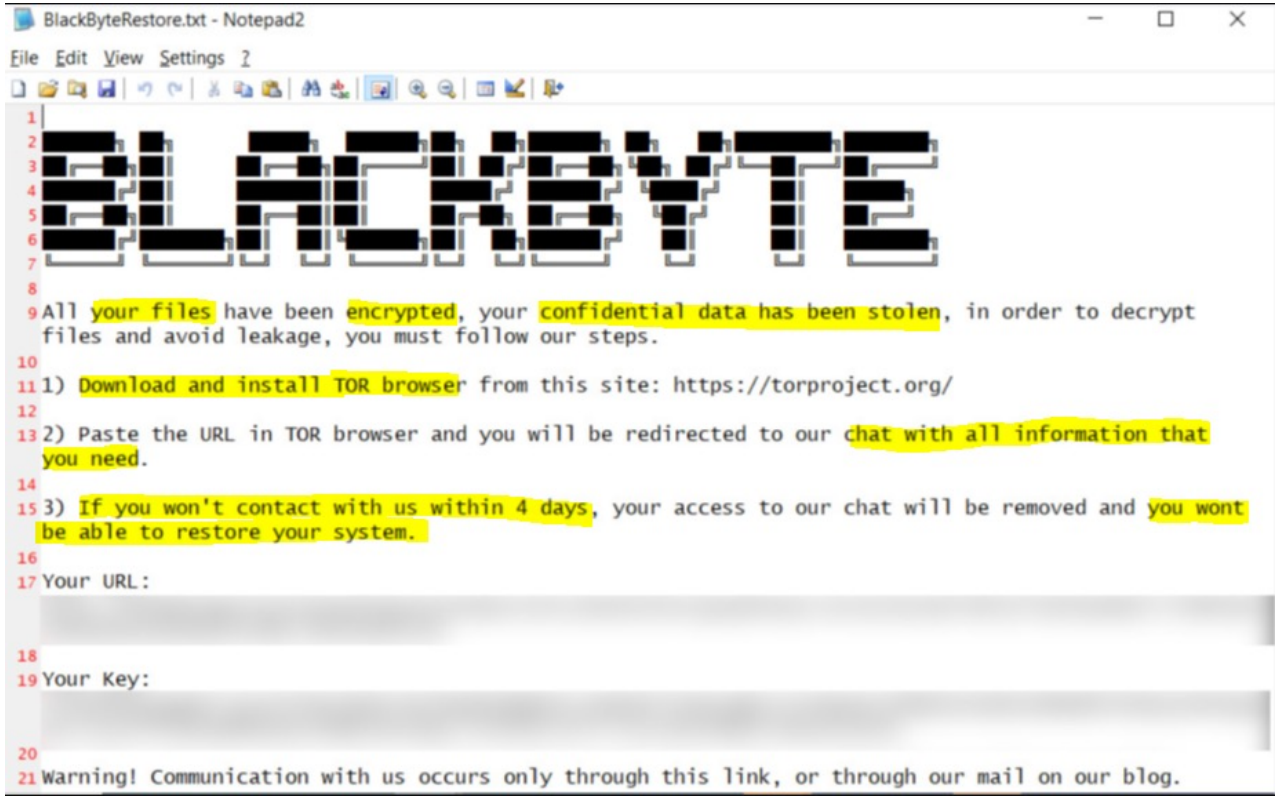
ATB. LAW

VERHANDELN MIT DEN ANGREIFERN?

ATB. LAW

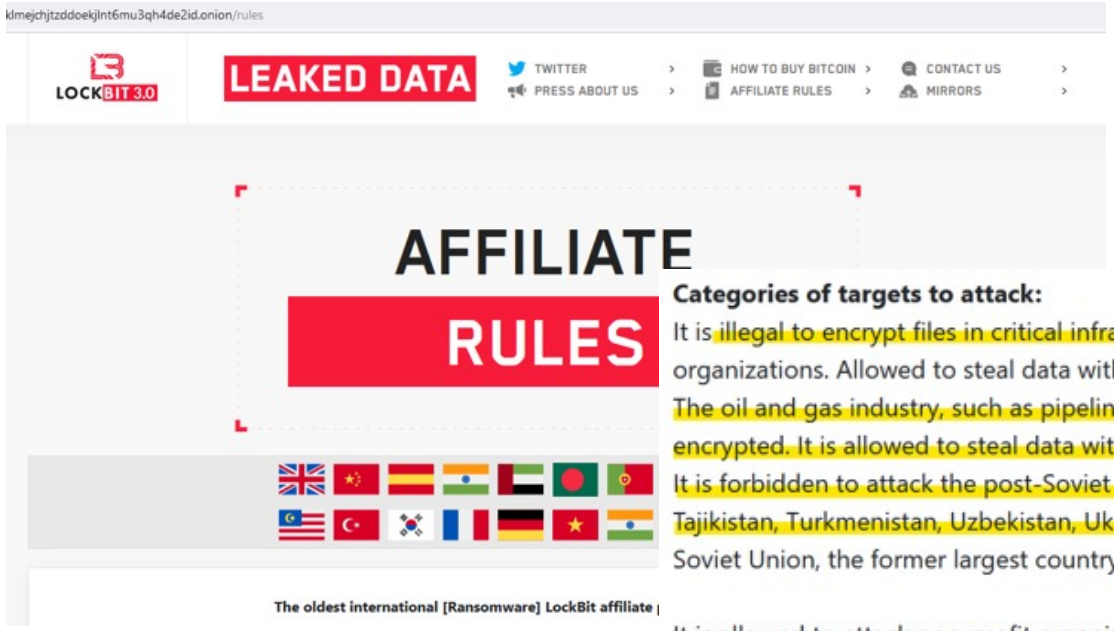
DARF/SOLL ICH VERHANDELN?

- NICHT STRAFBAR
- SINNVOLL?
  - Informationen
  - Zeit
  - Optionen



ATB. LAW

DARF/SOLL ICH VERHANDELN?



Categories of targets to attack:

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.

The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.

It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.

It is allowed to attack any educational institutions as long as they are private and have a revenue.

It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is

ATB. LAW

DARF/SOLL ICH VERHANDELN?

ATB. LAW

LÖSEGELD

ATB. LAW

DARF/SOLL ICH LÖSEGELD BEZAHLEN

- Sinnhaftigkeit -> Einzelfallabwägung
- Strafrechtliche Zulässigkeit
  - Untreue des Geschäftsführers
    - Zum Unternehmenswohl – „Business Judgement Rule“
    - Gesellschafterbeschluss
  - Beteiligung an einer kriminellen/terroristischen Vereinigung
    - Bereitstellung von Vermögenswerten (Lösegeld) = Beteiligung
    - Rechtfertigungs- und Entschuldigungsgründe

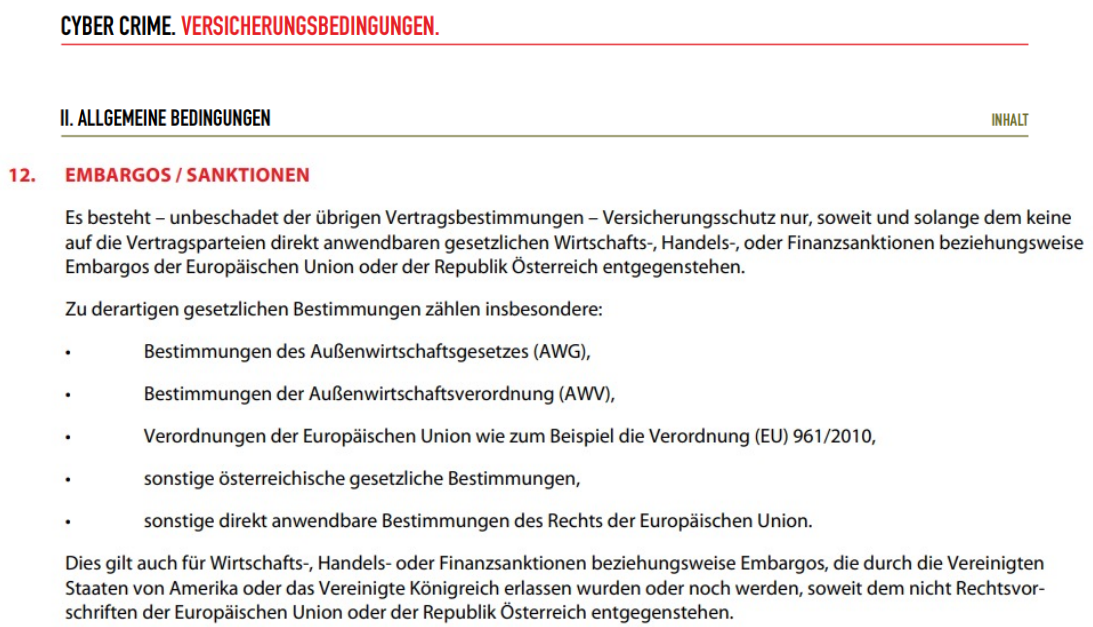
DOKUMENTATION !

ATB. LAW

DARF/SOLL ICH LÖSEGELD BEZAHLEN

- Sanktionslistenprüfung

DOKUMENTATION !



CYBER CRIME. VERSICHERUNGSBEDINGUNGEN.

II. ALLGEMEINE BEDINGUNGEN INHALT

12. EMBARGOS / SANKTIONEN

Es besteht – unbeschadet der übrigen Vertragsbestimmungen – Versicherungsschutz nur, soweit und solange dem keine auf die Vertragsparteien direkt anwendbaren gesetzlichen Wirtschafts-, Handels-, oder Finanzsanktionen beziehungsweise Embargos der Europäischen Union oder der Republik Österreich entgegenstehen.

Zu derartigen gesetzlichen Bestimmungen zählen insbesondere:

- Bestimmungen des Außenwirtschaftsgesetzes (AWG),
- Bestimmungen der Außenwirtschaftsverordnung (AWV),
- Verordnungen der Europäischen Union wie zum Beispiel die Verordnung (EU) 961/2010,
- sonstige österreichische gesetzliche Bestimmungen,
- sonstige direkt anwendbare Bestimmungen des Rechts der Europäischen Union.

Dies gilt auch für Wirtschafts-, Handels- oder Finanzsanktionen beziehungsweise Embargos, die durch die Vereinigten Staaten von Amerika oder das Vereinigte Königreich erlassen wurden oder noch werden, soweit dem nicht Rechtsvorschriften der Europäischen Union oder der Republik Österreich entgegenstehen.

ATB. LAW

Zusammengefasst

- Ransomwareangriffe sind auch rechtliche Herausforderungen
- Zeitdruck erfordert koordiniertes und effektives Handeln
- Dokumentation sämtlicher Entscheidungen ist wesentlich
- Man kann sich nicht 100% schützen, aber das (rechtliche) Risiko mit dem notwendigen Know-How minimieren

ATB. LAW

Vielen Dank für die Aufmerksamkeit!

Rechtsanwält:innen in Kooperation | Bauernmarkt 24, Top 15 | 1010 Wien | office@atb.law | www.atb.law