PYSA – Protokoll einer Ransomware-Attacke: Erfahrungsbericht der Universität Liechtenstein

Martin Häring, MSc

UNIVERSITÄT LIECHTENSTEIN

Zur eigenen Person…

Martin Häring, MSc

- Geb. 1983 in Feldkirch
- Studien der Informatik und des Prozessmanagements
- Langjährige Industrieerfahrung in den Bereichen Projekt- und Prozessmanagement sowie Leitung von Qualitätsmanagement und -sicherung
- Universität Liechtenstein:
  - Prozessmanager seit August 2020
  - Datenschutzbeauftragter seit Juli 2021
  - Leitung Prozessmanagement seit Mai 2022

STUNDE 0

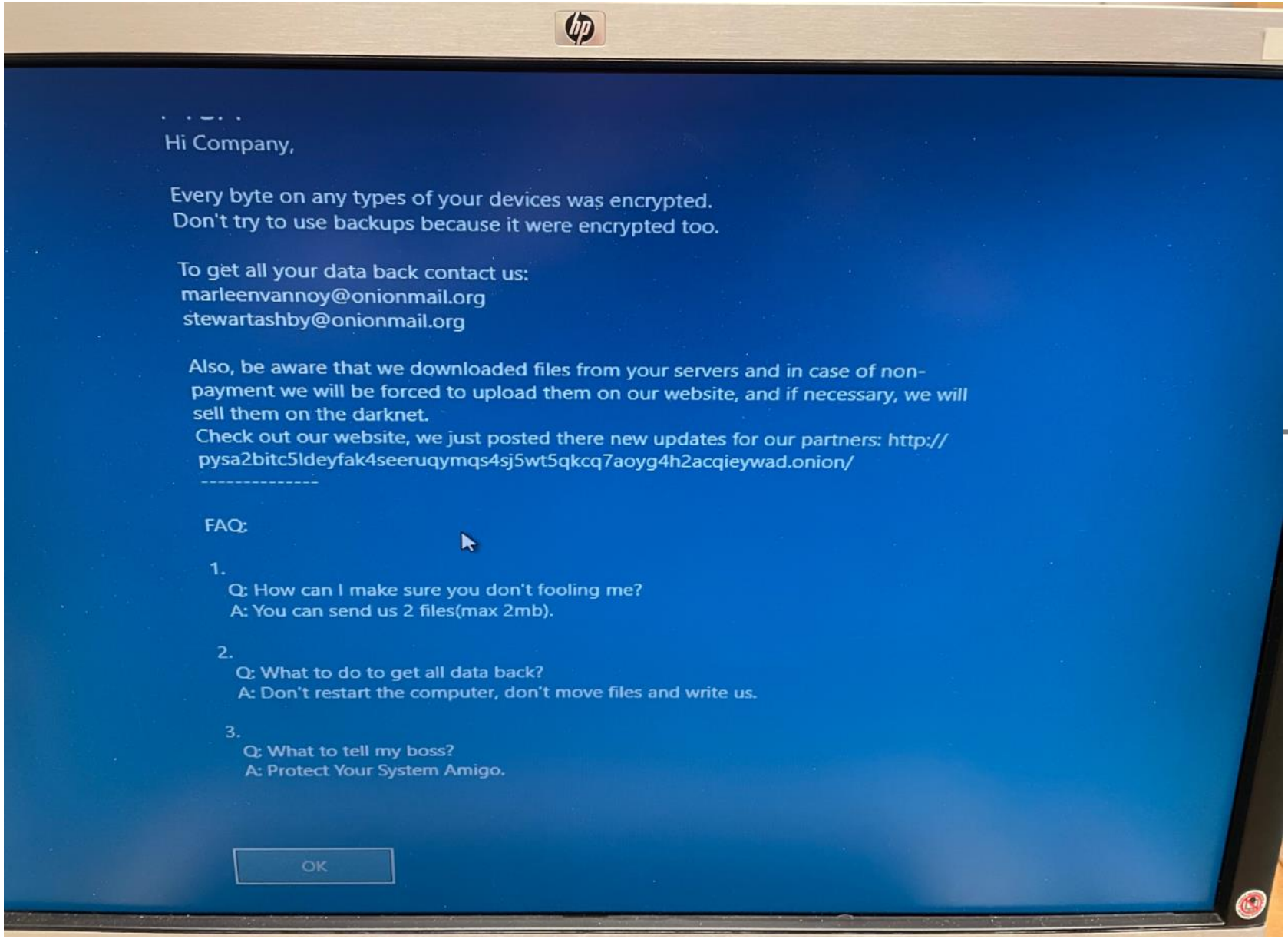
- **Netzausfall**
- **Server verschlüsselt**
- **PYSA-Meldung**

UNIVERSITÄT LIECHTENSTEIN

STUNDE 0

- **Netzausfall**
- **Server verschlüsselt**
- **PYSA-Meldung**

UNIVERSITÄT LIECHTENSTEIN


Hi Company,
Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.
To get all your data back contact us:
marleenvannoy@onionmail.org
stewartashby@onionmail.org
Also, be aware that we downloaded files from your servers and in case of non-payment we will be forced to upload them on our website, and if necessary, we will sell them on the darknet.
Check out our website, we just posted there new updates for our partners: http://pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h2acqieywad.onion/
FAQ:
1.
Q: How can I make sure you don't fooling me?
A: You can send us 2 files(max 2mb).
2.
Q: What to do to get all data back?
A: Don't restart the computer, don't move files and write us.
3.
Q: What to tell my boss?
A: Protect Your System Amigo.
OK

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- **Physische Trennung vom Internet**
- **Shutdown Server**
- **Kein Internet, E-Mail, Telefon, Applikationen, Daten**

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- Physische Trennung vom Internet
- Shutdown Server
- Kein Internet, E-Mail, Telefon, Applikationen, Daten

STUNDE 1

- **Meldungen DSB / Polizei**
- **Information an Rektorat**
- **Bildung Task-Force**
- **Vorläufige Meldung an Datenschutzstelle**

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- Physische Trennung vom Internet
- Shutdown Server
- Kein Internet, E-Mail, Telefon, Applikationen, Daten

STUNDE 1

- Meldungen DSB / Polizei
- Information an Rektorat
- Bildung Task-Force
- Vorläufige Meldung an Datenschutzstelle
- **Transparenz, aber nur relevante Information**
- **Zielgruppengerechte Kommunikation**
- **Sicherheit vor Geschwindigkeit**

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- Physische Trennung vom Internet
- Shutdown Server
- Kein Internet, E-Mail, Telefon, Applikationen, Daten

TAG 1

- **Externe und interne IT-Fachexpertise**
- **War Room**
- **Sicherung von Kommunikationskanälen (Website, etc.)**
- **Bericht an Universitätsrat und Regierung**
- **In der Nacht: Hinzuziehen von Ransomware-Experten**

STUNDE 1

- Meldungen DSB / Polizei
- Information an Rektorat
- Bildung Task-Force
- Vorläufige Meldung an Datenschutzstelle
- Transparenz, aber nur relevante Information
- Zielgruppengerechte Kommunikation
- Sicherheit vor Geschwindigkeit

UNIVERSITÄT LIECHTENSTEIN

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- Physische Trennung vom Internet
- Shutdown Server
- Kein Internet, E-Mail, Telefon, Applikationen, Daten

TAG 1

- Externe und interne IT-Fachexpertise
- War Room
- Sicherung von Kommunikationskanälen (Website, etc.)
- Bericht an Universitätsrat und Regierung
- In der Nacht: Hinzuziehen von Ransomware-Experten

STUNDE 1

- Meldungen DSB / Polizei
- Information an Rektorat
- Bildung Task-Force
- Vorläufige Meldung an Datenschutzstelle
- Transparenz, aber nur relevante Information
- Zielgruppengerechte Kommunikation
- Sicherheit vor Geschwindigkeit

WOCHEN 1 – 2

- **Information an Betroffene via Facebook, LinkedIn, Zeitungen, Website**
- **Wiederherstellung E-Mail und Telefonie**
- **Erste Ursachenforschung und Identifikation betroffener Systeme**
- **Backups und Syslogs verschlüsselt!**

UNIVERSITÄT LIECHTENSTEIN

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- Physische Trennung vom Internet
- Shutdown Server
- Kein Internet, E-Mail, Telefon, Applikationen, Daten

TAG 1

- Externe und interne IT-Fachexpertise
- War Room
- Sicherung von Kommunikationskanälen (Website, etc.)
- Bericht an Universitätsrat und Regierung
- In der Nacht: Hinzuziehen von Ransomware-Experten

WOCHE -2

- **Zugriff auf Netzwerk mit erbeuteten oder gekauften Zugangsdaten**
- **Zugriff erfolgte über Citrix (Applikation für Remote Work)**
- **Keine aktive Zwei-Faktor-Authentisierung auf diesem System**

CITRIX®

STUNDE 1

- Meldungen DSB / Polizei
- Information an Rektorat
- Bildung Task-Force
- Vorläufige Meldung an Datenschutzstelle
- Transparenz, aber nur relevante Information
- Zielgruppengerechte Kommunikation
- Sicherheit vor Geschwindigkeit

WOCHEN 1 – 2

- Information an Betroffene via Facebook, LinkedIn, Zeitungen, Website
- Wiederherstellung E-Mail und Telefonie
- Erste Ursachenforschung und Identifikation betroffener Systeme
- Backups und Syslogs verschlüsselt!

VOR MONATEN

- **Vermutlich Zugangsdaten von Studierenden erbeutet**
- **Verkauf im Darknet**

LINK	ACCESS TYPE	HEADQUARTERS	PHONE NUMBER	REVENUE	NUMBER OF EMPLOYEES	WEBSITE	ACTIVITY TYPE	LINE
citrix.uni.li	citrix	Vaduz, Vaduz, Liechtenstein		$61 Million	154	www.uni.li	Colleges & Universities, Education	190

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- Physische Trennung vom Internet
- Shutdown Server
- Kein Internet, E-Mail, Telefon, Applikationen, Daten

TAG 1

- Externe und interne IT-Fachexpertise
- War Room
- Sicherung von Kommunikationskanälen (Website, etc.)
- Bericht an Universitätsrat und Regierung
- In der Nacht: Hinzuziehen von Ransomware-Experten

WOCHE –2

- Zugriff auf Netzwerk mit erbeuteten oder gekauften Zugangsdaten
- Zugriff erfolgte über Citrix (Applikation für Remote Work)
- Keine aktive Zwei-Faktor-Authentisierung auf diesem System

CITRIX®

STUNDE 1

- Meldungen DSB / Polizei
- Information an Rektorat
- Bildung Task-Force
- Vorläufige Meldung an Datenschutzstelle
- Transparenz, aber nur relevante Information
- Zielgruppengerechte Kommunikation
- Sicherheit vor Geschwindigkeit

WOCHEN 1 – 2

- Information an Betroffene via Facebook, LinkedIn, Zeitungen, Website
- Wiederherstellung E-Mail und Telefonie
- Erste Ursachenforschung und Identifikation betroffener Systeme
- Backups und Syslogs verschlüsselt!

UNIVERSITÄT LIECHTENSTEIN

VOR MONATEN

- **Vermutlich Zugangsdaten von Studierenden erbeutet**
- **Verkauf im Darknet**

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- Physische Trennung vom

TAG 1

- Externe und interne IT-Fachexpertise
- War Room
- Sicherung von Kommunikationskanälen (Website, etc.)
- Bericht an Universitätsrat und

LINK	ACCESS TYPE	HEADQUARTERS	PHONE NUMBER	REVENUE	NUMBER OF EMPLOYEES	WEBSITE	ACTIVITY TYPE	LINE
citrix.uni.li	citrix	Vaduz, Vaduz, Liechtenstein		$61 Million	154	www.uni.li	Colleges & Universities, Education	190

- Remote Work)
- Keine aktive Zwei-Faktor-Authentisierung auf diesem System

- Transparenz, aber nur relevante Information
- Zielgruppengerechte Kommunikation
- Sicherheit vor Geschwindigkeit

- Erste Ursachenforschung und Identifikation betroffener Systeme
- Backups und Syslogs verschlüsselt!

WOCHE –2

STUNDE 1

WOCHEN 1 – 2

VOR MONATEN

- Vermutlich Zugangsdaten von Studierenden erbeutet
- Verkauf im Darknet

LINK	ACCESS TYPE	HEADQUARTERS	PHONE NUMBER	REVENUE	NUMBER OF EMPLOYEES	WEBSITE	ACTIVITY TYPE	LINE
citrix.uni.li	citrix	Vaduz, Vaduz, Liechtenstein		$61 Million	154	www.uni.li	Colleges & Universities, Education	190

WOCHE –2

- Zugriff auf Netzwerk mit erbeuteten oder gekauften Zugangsdaten
- Zugriff erfolgte über Citrix (Applikation für Remote Work)
- Keine aktive Zwei-Faktor-Authentisierung auf diesem System

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- Physische Trennung vom Internet
- Shutdown Server
- Kein Internet, E-Mail, Telefon, Applikationen, Daten

STUNDE 1

- Meldungen DSB / Polizei
- Information an Rektorat
- Bildung Task-Force
- Vorläufige Meldung an Datenschutzstelle
- Transparenz, aber nur relevante Information
- Zielgruppengerechte Kommunikation
- Sicherheit vor Geschwindigkeit

TAG 1

- Externe und interne IT-Fachexpertise
- War Room
- Sicherung von Kommunikationskanälen (Website, etc.)
- Bericht an Universitätsrat und Regierung
- In der Nacht: Hinzuziehen von Ransomware-Experten

WOCHEN 1 – 2

- Information an Betroffene via Facebook, LinkedIn, Zeitungen, Website
- Wiederherstellung E-Mail und Telefonie
- Erste Ursachenforschung und Identifikation betroffener Systeme
- Backups und Syslogs verschlüsselt!
- **Kontaktaufnahme mit Erpressern durch Experten (20 BTC)**

UNIVERSITÄT LIECHTENSTEIN

Negotation X
Dear, I've been contacted by the Univercity of Liechtenstein to contact you regarding the encryption proces of their network. What are the next steps in this pr
17 aug. 2021 15:24 (2 dagen geleden)

Marleen J Vannoy
You need to send 20 btc to our wallet to get decryption software and remove your sensitive data. Tor site: http://pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h
18 aug. 2021 14:42 (1 dag geleden)

Marleen J Vannoy
btc wallet: bc1q73ca94sjtkd0fteda495f6790ut5f3gqdn9r4h
18 aug. 2021 14:43 (1 dag geleden)

Negotation X
Hi Marleen, I will contact the customer, but this is really not an accebtable offer. they have 75 servers... Regards Geert Op wo 18 aug. 2021 om 14:43 schreef M
18 aug. 2021 16:18 (1 dag geleden)

Marleen J Vannoy
we will make a discount 30 percent if you pay today
18 aug. 2021 17:19 (1 dag geleden)

Negotation X
This amount is just to high!! They will never do this... Keep you in contact Op wo 18 aug. 2021 om 17:19 schreef Marleen J Vannoy <marleenvannoy@onionmail.org>:
18 aug. 2021 17:41 (1 dag geleden)

Marleen J Vannoy
aan mij
publish their data?
17:51 (3 uur geleden)

VOR MONATEN

- Vermutlich Zugangsdaten von Studierenden erbeutet
- Verkauf im Darknet

LINK	ACCESS TYPE	HEADQUARTERS	PHONE NUMBER	REVENUE	NUMBER OF EMPLOYEES	WEBSITE	ACTIVITY TYPE	LINE
citrix.uni.li	citrix	Vaduz, Vaduz, Liechtenstein		$61 Million	154	www.uni.li	Colleges & Universities, Education	190

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- Physische Trennung vom Internet
- Shutdown Server
- Kein Internet, E-Mail, Telefon, Applikationen, Daten

TAG 1

- Externe und interne IT-Fachexpertise
- War Room
- Sicherung von Kommunikationskanälen (Website, etc.)
- Bericht an Universitätsrat und Regierung
- In der Nacht: Hinzuziehen von Ransomware-Experten

WOCHEN 1 – 2

- **Fortlaufender Kontakt mit DSB**
- **Weitere Datenschutzverletzung**
- **Auflistung der wahrscheinlich betroffenen Systeme und Risikobewertung**

WOCHE –2

- Zugriff auf Netzwerk mit erbeuteten oder gekauften Zugangsdaten
- Zugriff erfolgte über Citrix (Applikation für Remote Work)
- Keine aktive Zwei-Faktor-Authentisierung auf diesem System

CITRIX®

STUNDE 1

- Meldungen DSB / Polizei
- Information an Rektorat
- Bildung Task-Force
- Vorläufige Meldung an Datenschutzstelle
- Transparenz, aber nur relevante Information
- Zielgruppengerechte Kommunikation
- Sicherheit vor Geschwindigkeit

WOCHEN 1 – 2

- Information an Betroffene via Facebook, LinkedIn, Zeitungen, Website
- Wiederherstellung E-Mail und Telefonie
- Erste Ursachenforschung und Identifikation betroffener Systeme
- Backups und Syslogs verschlüsselt!
- Kontaktaufnahme mit Erpressern durch Experten (20 BTC)

UNIVERSITÄT LIECHTENSTEIN

VOR MONATEN

- Vermutlich Zugangsdaten von Studierenden erbeutet
- Verkauf im Darknet

LINK	ACCESS TYPE	HEADQUARTERS	PHONE NUMBER	REVENUE	NUMBER OF EMPLOYEES	WEBSITE	ACTIVITY TYPE	LINE
citrix.uni.li	citrix	Vaduz, Vaduz, Liechtenstein		$61 Million	154	www.uni.li	Colleges & Universities, Education	190

WOCHE –2

- Zugriff auf Netzwerk mit erbeuteten oder gekauften Zugangsdaten
- Zugriff erfolgte über Citrix (Applikation für Remote Work)
- Keine aktive Zwei-Faktor-Authentisierung auf diesem System

CITRIX®

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- Physische Trennung vom Internet
- Shutdown Server
- Kein Internet, E-Mail, Telefon, Applikationen, Daten

STUNDE 1

- Meldungen DSB / Polizei
- Information an Rektorat
- Bildung Task-Force
- Vorläufige Meldung an Datenschutzstelle
- Transparenz, aber nur relevante Information
- Zielgruppengerechte Kommunikation
- Sicherheit vor Geschwindigkeit

TAG 1

- Externe und interne IT-Fachexpertise
- War Room
- Sicherung von Kommunikationskanälen (Website, etc.)
- Bericht an Universitätsrat und Regierung
- In der Nacht: Hinzuziehen von Ransomware-Experten

WOCHEN 1 – 2

- Information an Betroffene via Facebook, LinkedIn, Zeitungen, Website
- Wiederherstellung E-Mail und Telefonie
- Erste Ursachenforschung und Identifikation betroffener Systeme
- Backups und Syslogs verschlüsselt!
- Kontaktaufnahme mit Erpressern durch Experten (20 BTC)

WOCHEN 1 – 2

- Fortlaufender Kontakt mit DSB
- Weitere Datenschutzverletzung
- Auflistung der wahrscheinlich betroffenen Systeme und Risikobewertung
- **Erhöhung der Sicherheit und Passwort-Änderungen (auch privat)**
- **Wiederherstellung einzelner IT-Systeme**
- **Entscheidung zum kompletten Neu-Aufbau der IT-Infrastruktur**

UNIVERSITÄT LIECHTENSTEIN

VOR MONATEN

- Vermutlich Zugangsdaten von Studierenden erbeutet
- Verkauf im Darknet

LINK	ACCESS TYPE	HEADQUARTERS	PHONE NUMBER	REVENUE	NUMBER OF EMPLOYEES	WEBSITE	ACTIVITY TYPE	LINE
citrix.uni.li	citrix	Vaduz, Vaduz, Liechtenstein		$61 Million	154	www.uni.li	Colleges & Universities, Education	190

STUNDE 0

- Netzausfall
- Server verschlüsselt
- PYSA-Meldung

- Physische Trennung vom Internet
- Shutdown Server
- Kein Internet, E-Mail, Telefon, Applikationen, Daten

TAG 1

- Externe und interne IT-Fachexpertise
- War Room
- Sicherung von Kommunikationskanälen (Website, etc.)
- Bericht an Universitätsrat und Regierung
- In der Nacht: Hinzuziehen von Ransomware-Experten

WOCHEN 1 – 2

- Fortlaufender Kontakt mit DSB
- Weitere Datenschutzverletzung
- Auflistung der wahrscheinlich betroffenen Systeme und Risikobewertung
- Erhöhung der Sicherheit und Passwort-Änderungen (auch privat)
- Wiederherstellung einzelner IT-Systeme
- Entscheidung zum kompletten Neu-Aufbau der IT-Infrastruktur

WOCHE –2

- Zugriff auf Netzwerk mit erbeuteten oder gekauften Zugangsdaten
- Zugriff erfolgte über Citrix (Applikation für Remote Work)
- Keine aktive Zwei-Faktor-Authentisierung auf diesem System

CITRIX®

STUNDE 1

- Meldungen DSB / Polizei
- Information an Rektorat
- Bildung Task-Force
- Vorläufige Meldung an Datenschutzstelle
- Transparenz, aber nur relevante Information
- Zielgruppengerechte Kommunikation
- Sicherheit vor Geschwindigkeit

WOCHEN 1 – 2

- Information an Betroffene via Facebook, LinkedIn, Zeitungen, Website
- Wiederherstellung E-Mail und Telefonie
- Erste Ursachenforschung und Identifikation betroffener Systeme
- Backups und Syslogs verschlüsselt!
- Kontaktaufnahme mit Erpressern durch Experten (20 BTC)

WOCHEN 3 – 10

- **Planung / Start Wiederaufbau**
- **Benachrichtigung der betroffenen Personen nach Art. 34 DSGVO**
- **Zahlreiche Rückfragen betroffener Personen**
- **Auskunftsbegehren**
- **Löschbegehren**
- **Vollständige Meldung Datenschutzverletzung einen Monat nach dem Ereignis**

UNIVERSITÄT LIECHTENSTEIN

Learnings / Empfehlungen

Technische Learnings

- **Präventionsmassnahmen**
  - Durchgängige Zwei-Faktor-Authentisierung
  - Penetrationstests
  - Darknet-Screening

- **Sofort- und Korrekturmassnahmen**
  - Internet trennen
  - KEIN Shutdown der Server
  - Externe Expertise
  - Kompletter Wiederaufbau der IT-Landschaft

Organisatorische Learnings

- **Anpassung Backup-Strategie**

- **Task Force:**
  - Interne IT
  - Geschäftsleitung
  - Kommunikation
  - Business Continuity
  - Datenschutzbeauftragte/r
  - Externe Fachexpertise (Ransomware)
  - IKS- und Risikomanagement

- **„War Room“**

Organisatorische Learnings

- **Falls Kommunikation mit Erpressenden → extern**

- **Risikoentscheid: Lösegeld-Forderung**
  - > Alle Varianten und Kombinationen möglich: Zahlung / Entschlüsselung / erneute Verschlüsselung / Veröffentlichung / Verkauf der Daten

- **Internes Notfallkonzept (Business Continuity)**

- **Datenschutz: Informierung betroffener Personen**
  - > Self-Assessment mit hoher Komplexität
  - > Relevanter Informationsgewinn vs. „unverzügliche Meldung“
  - > Back-Up Verarbeitungsverzeichnis

UNIVERSITÄT
LIECHTENSTEIN