Das Forum für ICT im Gesundheitswesen
Le forum pour les TIC dans le système de santé

@eHealthSummit
@read42news
www.ehealthsummit.ch

SWISS eHEALTH SUMMIT 2017 HIMSS Europe

SGMI SSIM SSMI
Schweizerische Gesellschaft für Medizinische Informatik
Société Suisse d'Informatique Médicale
Società Svizzera d'Informatica Medica
Swiss Society for Medical Informatics

SwissTech Convention Center, Lausanne
21.-22. September 2017

Anatomie eines Cyberangriffes

Dr. med. Stefan Hunziker, eMBA UZH, Luzerner Kantonsspital

In cooperation with

ehealthsuisse
IHE SUISSE Integrating the Healthcare Enterprise
pharmaSuisse
VGIch
HIMSS CHiME INTERNATIONAL

AGENDA

- Vorbemerkung: Alltäglicher Wahnsinn
- Zeitlicher Ablauf
- Auswirkungen
- Wie handeln
- Learnings
- Künftiger Umgang mit Cyberrisiken

Von: "USPS Delivery" <usps@usdelivery.com>
An: <stefan.hunziker@luks.ch>
Datum: 31.05.2017 17:29
Betreff: Your package 421131752 has been returned!

Dear client,

Our courier was not able to deliver the package you sent on May 19th, 2017 because nobody wa
The package has been returned to our office after three failed delivery attempts.
Please visit the link below to view the delivery invoice, including the tracking number and the addr

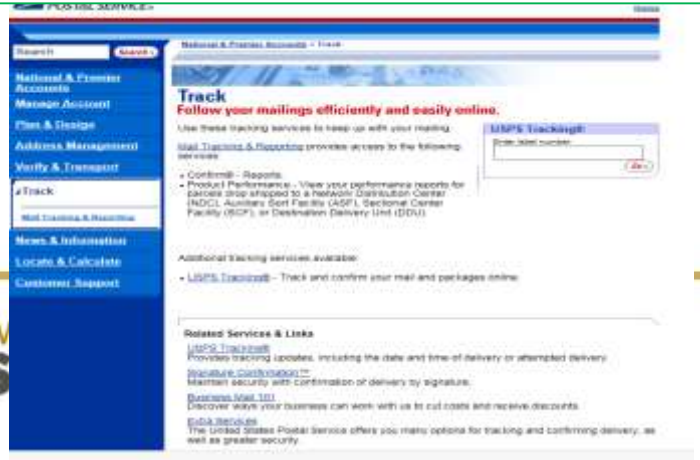
https://www.usps.com/track/invoice.aspx?package_id=4 21131752&acc=stefar

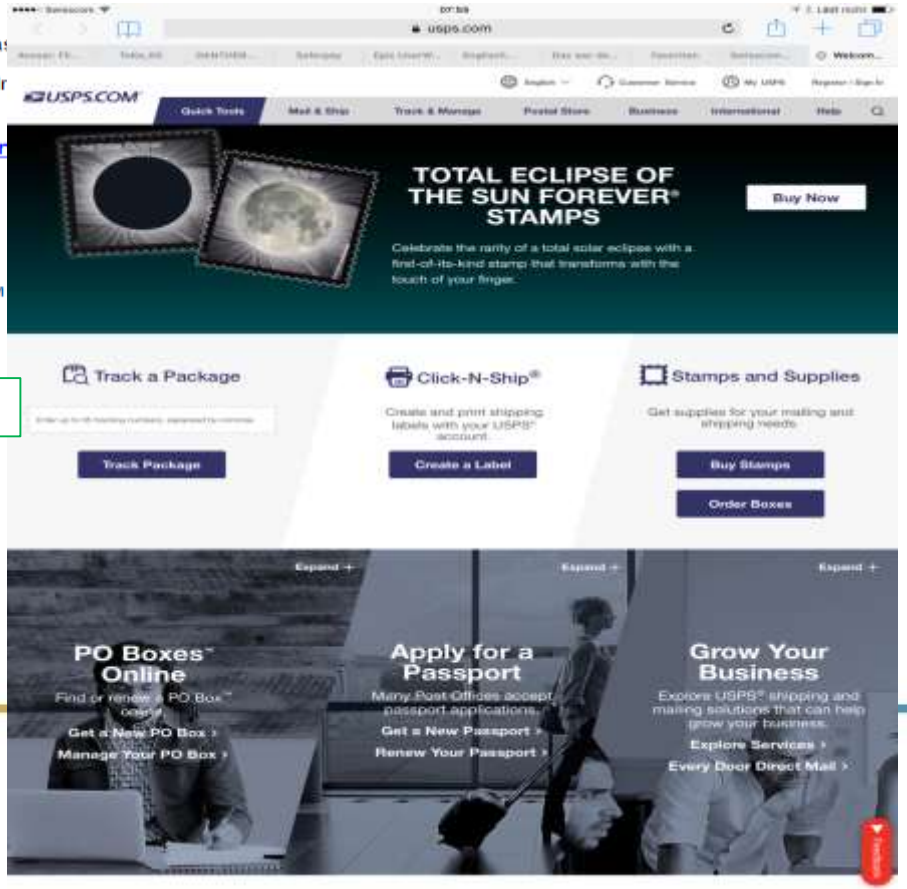
To reclaim your package, please visit our office with a printed copy of the invoice above.

Thank you

Thanks & Regards ,**Call:** 1-800-ASK-USPS® (1-800-275-8777) Monday -Friday 8 AM - 8:30 PM ET Saturday 8 AM

https://www.usps.com/nationalpremieraccounts/trackmailing.htm





65 Ergebnisse in 'Main'.

Ergebnisse anzeigen: Nach Datum (letzte Änderung)

Suchen nach: USPS Delivery | Suchen | Ergebnisliste löschen

Created	From	To
31.05.2017 21:34:40	"USPS Delivery" <usps@usdelivery.com>	
31.05.2017 20:21:10	"USPS Delivery" <usps@usdelivery.com>	
31.05.2017 20:03:56	"USPS Delivery" <usps@usdelivery.com>	
31.05.2017 19:44:42	"USPS Delivery" <usps@usdelivery.com>	
31.05.2017 19:08:36	"USPS Delivery" <usps@usdelivery.com>	
31.05.2017 18:18:52	"USPS Delivery" <usps@usdelivery.com>	
31.05.2017 17:57:09	"USPS Delivery" <usps@usdelivery.com>	
31.05.2017 17:49:01	"USPS Delivery" <usps@usdelivery.com>	
31.05.2017 17:46:17	"USPS Delivery" <usps@usdelivery.com>	
31.05.2017 17:29:18	"USPS Delivery" <usps@usdelivery.com>	<stefan.hunziker@luks.ch>
14.05.2017 05:21:58	"USPS Delivery" <gaykyboh37354@jayasoftwares.com>	
14.05.2017 02:54:03	"USPS International" <iqytkynu36276347@mascord.com>	
14.05.2017 01:56:58	"USPS Priority" <tawusoro53@seuprodutonaweb.com.br>	
14.05.2017 01:53:58	"USPS Priority Delivery" <xji76338344@covise.pt>	

17 Min.

ZEITLICHER ABLAUF

- Cryptolocker- Befall (Zepto)
- E-Mailanhang via privatem Webmail
- Start Datenverschlüsselung

Cryptolockerbefall (Zepto)

31.08.2016
16.35 Uhr

31.08.2016
16.55 Uhr

Stopp Datenverschlüsselung

- Mitarbeiter/in fährt PC he
- Stopp Datenverschlüsselung
- 6500 verschlüsselte Dateien
- Patientensicherheit nicht beeintrachtigt

Störungsmeldung IT-ServiceDesk geht ein

- IT bemerkt dadurch Cryptolockerbefall
- Notfallprozess wird gestartet

Start Notfallprozess

01.09.2016
08:45 Uhr

01.09.2016
09.00 Uhr

- Erstes Meeting Krisenstab
- Start Sofortmassnahmen
- Auslösen übergeordneter Krisenalarm

Start Notfallbewältigung

- Datenwiederherstellung abgeschlossen
- Rückkehr in Normalbetrieb
- Auflösen Krisenstab

Rückkehr in Normalbetrieb

01.09.2016
21.00 Uhr

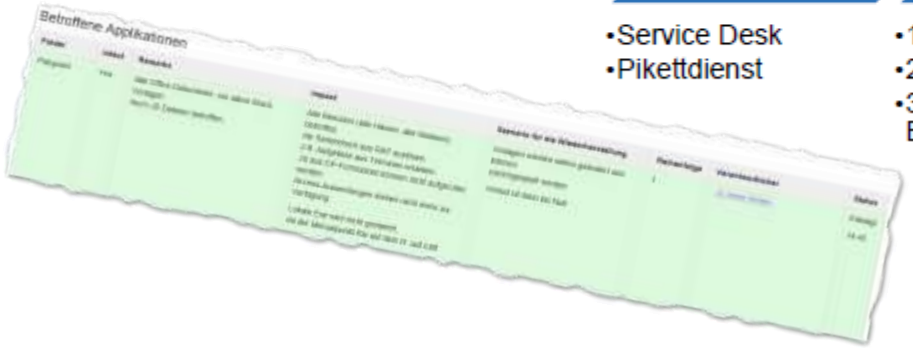
02.09.2016
14.00 Uhr

Eingang erster Medienanfragen …

Zeitachse

MAJOR INCIDENT

Auslöser	Eskalation	Analyse und Behebung	Abschluss
•Service Desk •Pikettdienst	•1. Service Desk •2. Major Manager •3. Hierarchische Eskalation	•Kommunikation •Aktivitäten zur Störungsbehebung	•Workaround steht •Review gemacht •alles dokumentiert

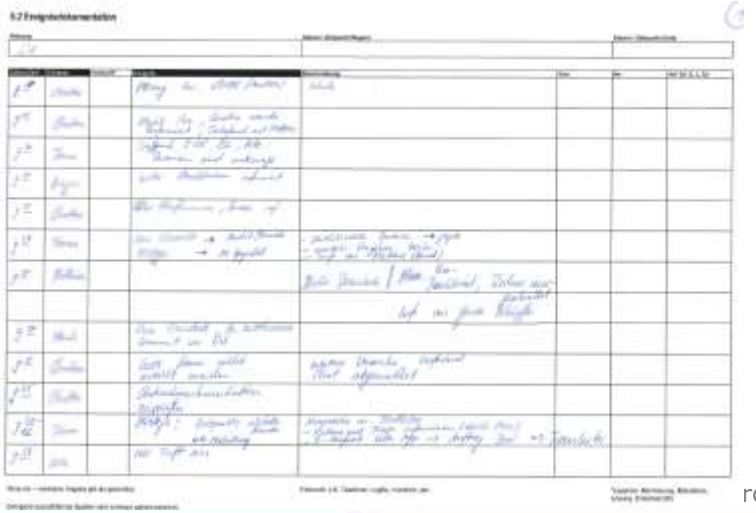


Protokoll After Review Action: 15.09.2016 (Sitzungszimmer Haus 4)

Anwesend: [redacted]

[redacted] Vorstellung der Präsentation → 2 Anträge sicherheitstechnisch an GLA → Antrag muss über [redacted] laufen.

Ablauf 01.09.2016:



AUSWIRKUNGEN

«Kleiner Schaden» (mehrere 10’000.-), aber …

Computervirus im Luzerner Kantonsspital

Veröffentlicht am 06. September 2016 9:34 — Letzte Aktualisierung 07. September 2016 15:16

Ein Computervirus gelang in das System des Luzerner Kantonsspitals (PD)

Auf einem Rechner des LUKS wurde ein Schädling festgestellt. Schäden entstanden keine.

Bild: http://www.lastwordonnothing.com

WAS MACHT MAN IN DIESEM MOMENT…

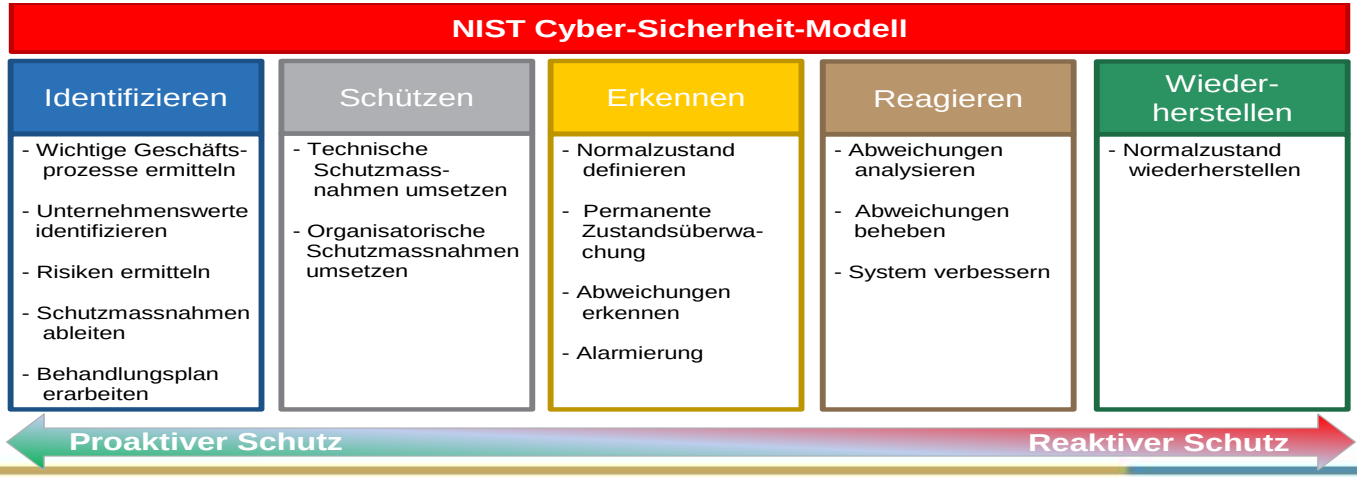
- Krisenstab einberufen
  - Entscheidungsfähigkeit sicherstellen (z.B. IT-Systeme herunterfahren / auf Papierbetrieb umstellen)
  - Ressourcen für Gegenmassnahmen zur Verfügung haben
- Sofortmassnahmen
  - Ausbreitung verhindern (Dateiendung Zepto auf Netzlaufwerken sperren)
  - Schwachstelle lokalisieren und beheben
  - Spezialisten anfordern (z.B. Forensiker)

LEARNINGS

- Sicherheit braucht den Rückhalt des Top-Managements
- Proaktive Schutzmassnahmen reichen heute nicht mehr aus (zum Infektions-Zeitpunkt haben 11 von 56 getesteten Virenscannern diese Schadsoftware erkannt)
- Private Webmailzugänge sind heute gesperrt (Risikobetrachtung)
- Technische Massnahmen sind wichtig – das richtige Verhalten der Mitarbeitenden ist wichtiger (Awareness)

KÜNFTIGER UMGANG MIT CYBERRISIKEN

- Konzeptioneller Ansatz
- Bessere Balance zwischen proaktiven / reaktiven Schutzmassnahmen
- In Abstimmung mit dem Business / der Unternehmensleitung



HERZLICHEN DANK

«Luzerner Kantonsspital – Wir helfen Ihnen sicher»

LUKS Luzern

LUKS Sursee

LUKS Wolhusen

Luzerner Höhenklinik Montana

Dr. med. S. Hunziker, Executive MBA UZH

Facharzt Chirurgie FMH
Wirtschaftsinformatiker FH
Luzerner Kantonsspital

stefan.hunziker@luks.ch

☏ +41 41 205 25 24