Security Nightmares

Ein Blick des EDUCV auf Sicherheits-Probleme und Albträume im letzten Jahr

EDUCV

- Der EDUCV ist „eine Arbeitsgruppe operativer Informationssicherheitsteams, insbesondere Computer Emergency Response Teams (CERTs) und Computer Security Incident Response Teams (CSIRTs), deutscher Hochschulen, Lehr- und Forschungseinrichtungen.“

Kurzinformation

- Gründung als Subverbund des Deutschen CERT-Verbundes
- regelmäßiger Informations- und Erfahrungsaustausch
- Unterstützung sicherheitstechnischer Untersuchungen
- Konzeption und Entwicklung von Sicherheitslösungen

ProxyLogon

ProxyLogon

- Wurmfähige unauthentifizierte Lücke in Microsoft Exchange
- Sehr leichte Ausnutzung möglich
- Sehr kurzer Zeitabstand zwischen Patch und verfügbarem Exploit Code
- Bei näherer Analyse von Systemen fanden sich mehrere erfolgreiche Angriffe sowie eine Unzahl an Scans
  - Dadurch war es sehr schwierig, erfolgreiche Angriffe von Scans zu unterscheiden
  - Uns sind mehrere kleine Exchange Systeme bekannt, die auf ein Backup zurückgesetzt werden mussten

Zu spät gepatchte Systeme galten schon nach einem Tag als potentiell übernommen!

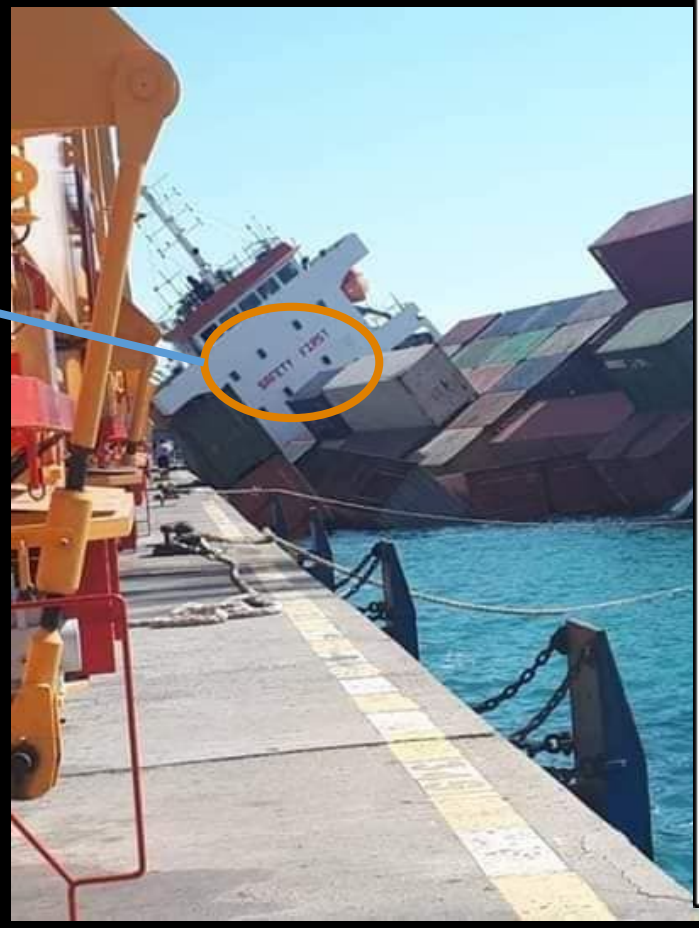
Print Nightmare

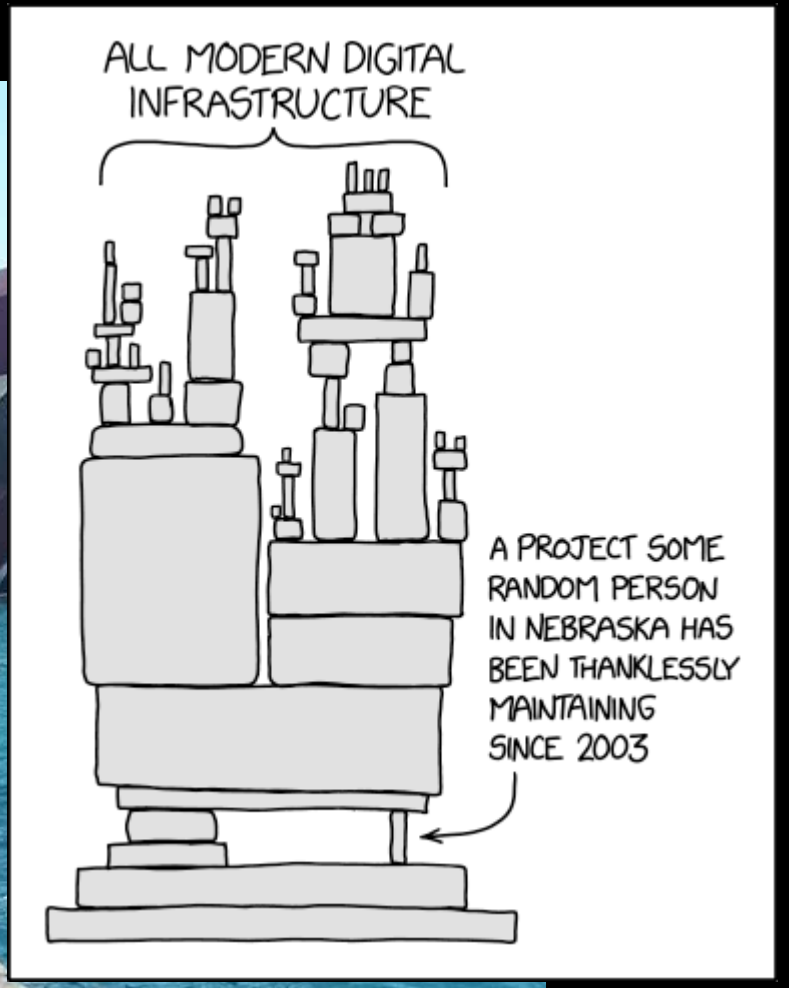
Das papierlose Büro oder PrintNightmare

- Treiber-Installation erfolgte mehr oder weniger ungeprüft mit SYSTEM Rechten
- Ermöglichte das Ausführen von Schadcode
- „Monatelange“ Patche, die immer wieder das Drucken behindert haben
- Trotz Einspielen der Patches wurde teilweise das Drucken verhindert und musste durch Anpassen der Konfiguration wieder ermöglicht werden

Reines Patchen hat hier nicht mehr gereicht, um das Problem zu beheben

Supply Chain





Supply Chain (The Nightmare Before Christmas)

- Wir haben mit dieser Präsentation vor dem 09.12. angefangen
- Die Supply Chain Folie sollte sich zu dem Zeitpunkt auf Dinge wie Solarwinds beziehen…
- Dann kam Log4Shell…
  - Fast überall integriert (Firewall, Backup Server, Minecraft??)
  - Etwas, das per Definition mit untrusted User Input arbeitet
  - Schwer zu finden, da in der Regel als Bundle in 3rd-Party Software

Patch NOW!

Apple products vulnerable to FORCEDENTRY zero-day attack – patch now!

Chrome zero-day, hot on the heels of Microsoft's IE zero-day. Patch now!

Call to Patch: Zero Day Discovered in [illegible] Help Desk Platform

Apache fixes actively exploited zero-day vulnerability, patch now

Chrome [illegible] day browser bug [illegible] – patch now!

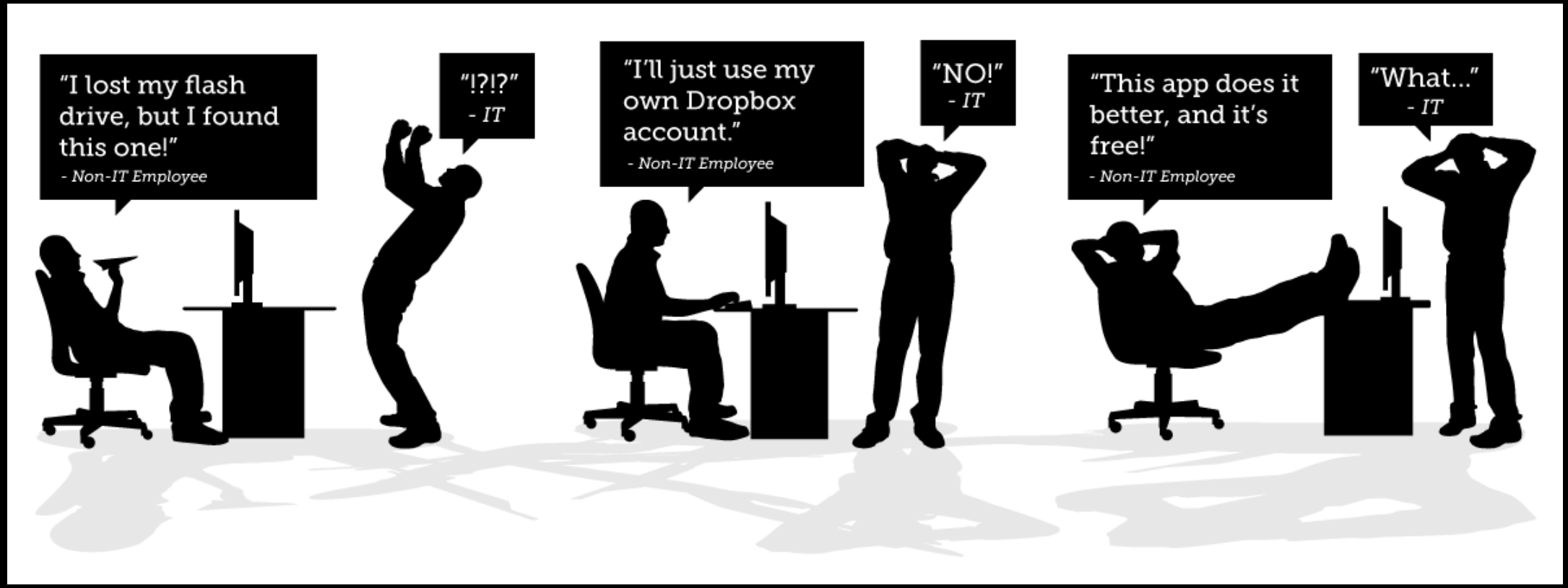
6 zero-days make this a 'Patch Now' Patch Tuesday

Alles brennt (Patch diese Webanwendung jetzt!)

Generelles Problem der Patch „Dringlichkeit“ kontra Zuständigkeit

- „Kollege is´ in Urlaub“
- „HiWi, der das aufgesetzt hat, arbeitet seit `nem Jahr nicht mehr hier“
- „Aber das Ding auf`m Schreibtisch leuchtet noch“
- „Soll ich das ausstecken?“
- „Das weiß ich doch nicht, wo das ist“
- „Der hat keine Vertretung!?“

Remote Arbeit
(Überall diese Schatten IT)



Ransom Attacken

- Auch dieser Jahr weiterhin Ransom Angriffe
  - Kaspersky spricht von ~370.000 Angriffen im Zeitraum von November 2020-Oktober 2021
- Extrem wirksam/schädigend
- Mittlerweile auch begleitet durch Datenexfiltration
- „Colonial Pipeline Attack“ von rEvil weltweit in den Nachrichten

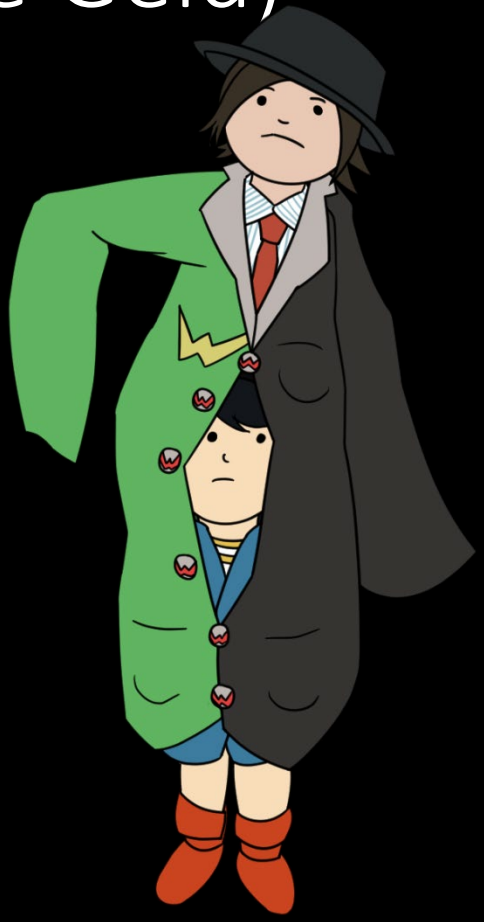
- Wenn sehr gut gesicherte Systeme Opfer solcher Angriffe werden – wie sollen wir uns mit unseren Mitteln dagegen dauerhaft erfolgreich schützen?

CEO Fraud
(Trust me – Ich brauche nur eben x Google Geld)

- Verbesserung der Ansprache

> Ich bin gerade in einem Meeting, deshalb kontaktiere ich Sie hier. Ich hätte Sie anrufen sollen, aber Telefonieren ist nicht erlaubt. Ich brauche Sie, um mir bei etwas Dringlichem zu helfen!

- Immer wieder Fälle mit echten Schäden
  - Schäden in Höhe von ~500€ pro Fall
- Schäden oft bei neuen Mitarbeitern und in Bereichen mit starkem Hierarchiegefälle



From: Prof. Dr.-ing ********** <headgroup001@gmail.com<mailto:headgroup001@gmail.com>>
Subject: Are you available?

Hello,

I need a favor from you kindly email me back as soon as possible.

Regards,
Prof. Dr.-ing **********
Director

Sent from my iPad

Hello, Professor,

Yes, I am available now.

Dear **********, Thank you for getting back to me. I need your assistance to get some gift cards from any store around now.There are some prospects i need to send Gift Cards today but I can't do that right now because I'm currently busy in the Hospital attending to my friend who's critically ill .Let me know if its possible to get them right now, so i can tell you which products i would need and what amount. I'll reimburse you.
Thanks.

Dear Professor,

My apartment is very close to the Hauptbahnhof, I can go buy the cards. Should I bring them back to <Name des Instituts>?

Dear **********, I need 4 qty of Google play gift cards at €200.00 each card When purchased, scratch-off the strip at the back of each card to reveal the codes,then send me clear and bold pictures of all the cards here so i can easily forward them to the prospects,before leaving the store and I'll need you to wait by the store while I wait for confirmation of all the codes.Keep the physical cards and receipt for reference purpose.
Thanks.

Dear Professor,

I am so sorry but 4 cards, each with 200 euro, could probably more than the limit I can use with my ********** Bank card for direct purchasing, it has a limitation for the student account and I haven't update with the bank. Is there any other way I can help?

Sorry again.

Dear **********, Kindly let me know how much you can purchase at the moment.
Thanks.

Dear Professor,

It's a 300 euro perday withdraw limits and 600 euro permonth for direct purchasing, not with online transfer.

Okay, Kindly go ahead with the 300 euro purchase and get back to me as soon as possible.
Thanks.

Eine halbe Stunde später...

Dear **********, You're yet to get back to me concerning the gift cards, Kindly get back to me as soon as possible.
Thanks.

Dear Professor,

Please check the card. The code on the top is

****

I tried with several times but only succeed with €200 payment. Sorry

With best wishes

Dear **********, Got them. Thanks so much for your time and kindness. But I want you to do me a last favor for me because the prospect made me realize the cards are still not enough for what they're needed for and I would like you to get them complete if not today you can complete them tomorrow so i can reimburse you and add a compensation to the stressed you gone through for me.
Thanks.

Dear Professor,

I can’t pay that much for one time today, then I can’t get them all in one time tomorrow. With all do respects, If that’s urgent, wouldn’t it be better if you ask someone else?

Best,
****

Dear **********, Not too late if you could try to get some tomorrow.
Thanks.

Empfehlung für die Zukunft

Der EDUCV besteht aus:

- DFN-CERT, Hamburg
- KIT-CERT, Karlsruhe
- WWU-CERT, Münster
- RUS-CERT, Stuttgart
- TUD-CERT, Dresden
- GU-CERT, Frankfurt
- FUB-ART, Berlin
- ZIM-CERT, Duisburg/Essen
- JMU-CERT, Würzburg

Sie finden uns unter

https://www.educv.de