UPS WE DID AGAIN... ALEBO ČO NEROBIŤ V KOMUNIKÁCII POČAS BEZPEČNOSTNÉHO INCIDENTU?

Daniel Chromek, CISO

Digital Security
Progress. Protected.

&

SME KONFERENCIE

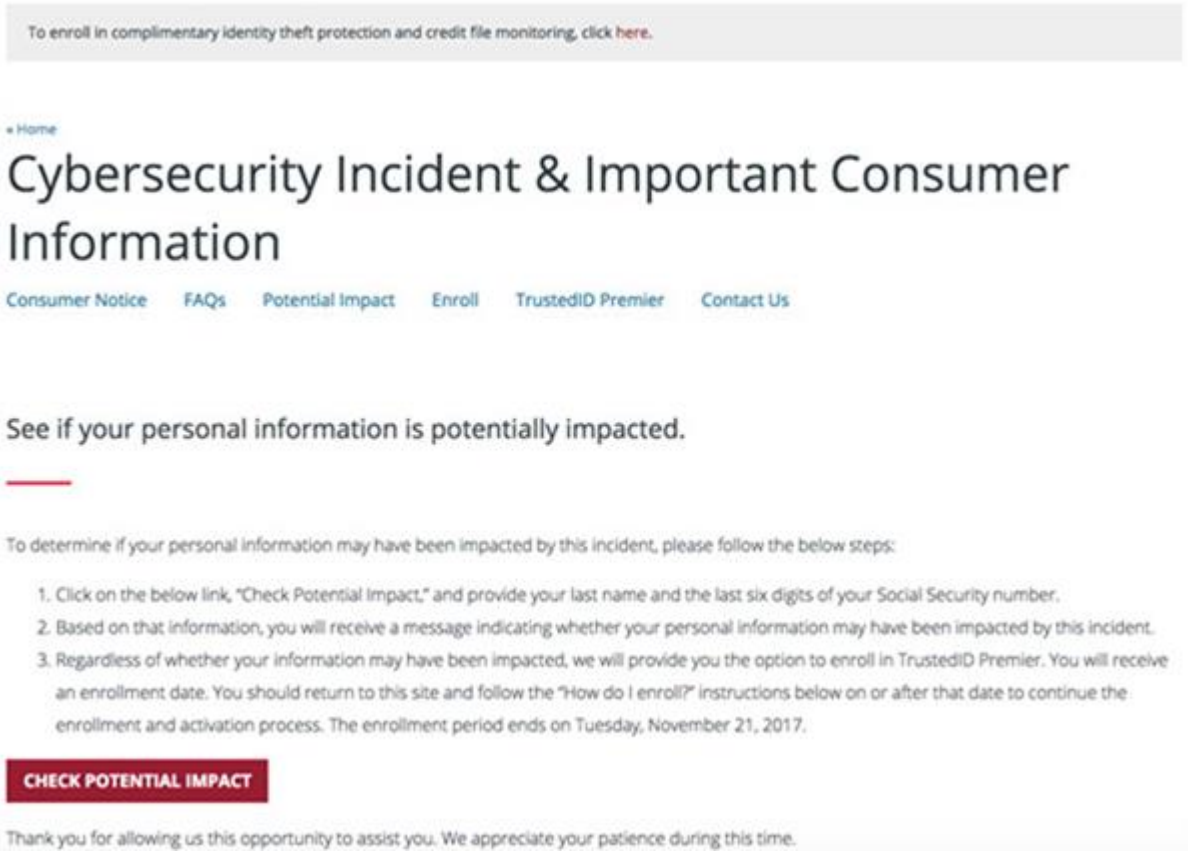
:~$ whoami && cat agenda.txt

- 15+ rokov v bezpečnosti
- @ESET od 2009
- ESET HQ CISO
- Zodpovedný za risk management, riadenie bezpečnosti a compliance (ISO 27001, ZoKB)

- Bol raz jeden incident
- Dlhé cesty a dlhé komunikačné rúrky
- Tikajúce hodinky
- Oslík zo Shreka
- Možné riešenia

Kde bolo, tam bolo…

Bol raz jeden incident...


To enroll in complimentary identity theft protection and credit file monitoring, click here.

« Home

Cybersecurity Incident & Important Consumer Information

Consumer Notice FAQs Potential Impact Enroll TrustedID Premier Contact Us

See if your personal information is potentially impacted.

To determine if your personal information may have been impacted by this incident, please follow the below steps:

1. Click on the below link, "Check Potential Impact," and provide your last name and the last six digits of your Social Security number.
2. Based on that information, you will receive a message indicating whether your personal information may have been impacted by this incident.
3. Regardless of whether your information may have been impacted, we will provide you the option to enroll in TrustedID Premier. You will receive an enrollment date. You should return to this site and follow the "How do I enroll?" instructions below on or after that date to continue the enrollment and activation process. The enrollment period ends on Tuesday, November 21, 2017.

CHECK POTENTIAL IMPACT

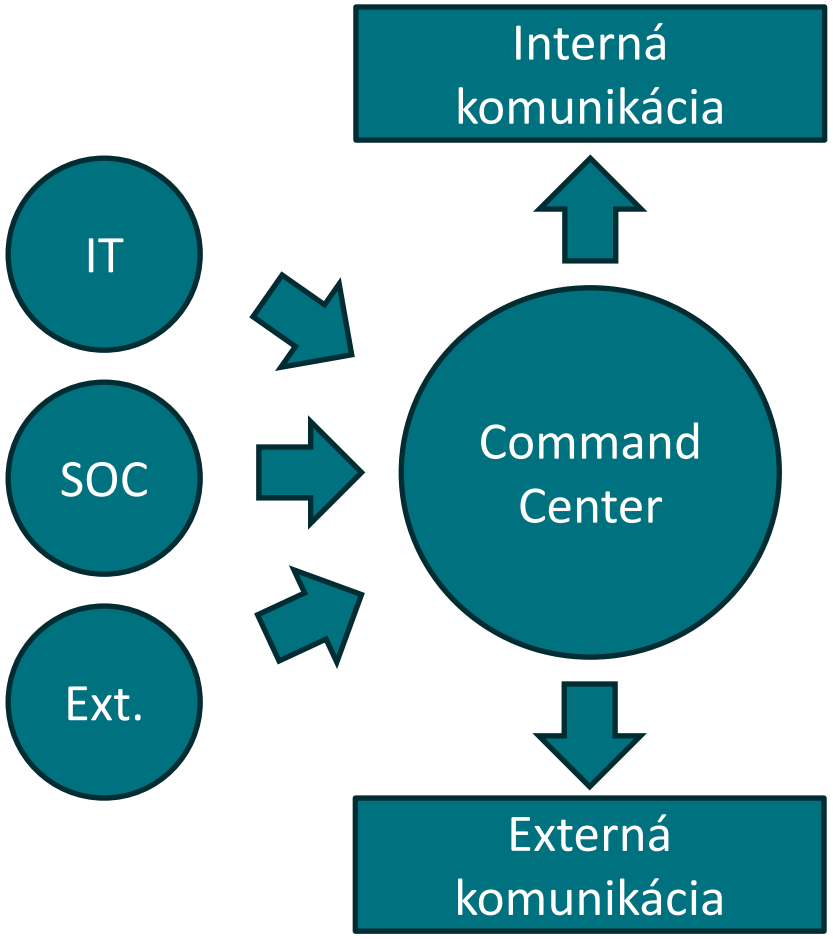
Thank you for allowing us this opportunity to assist you. We appreciate your patience during this time.

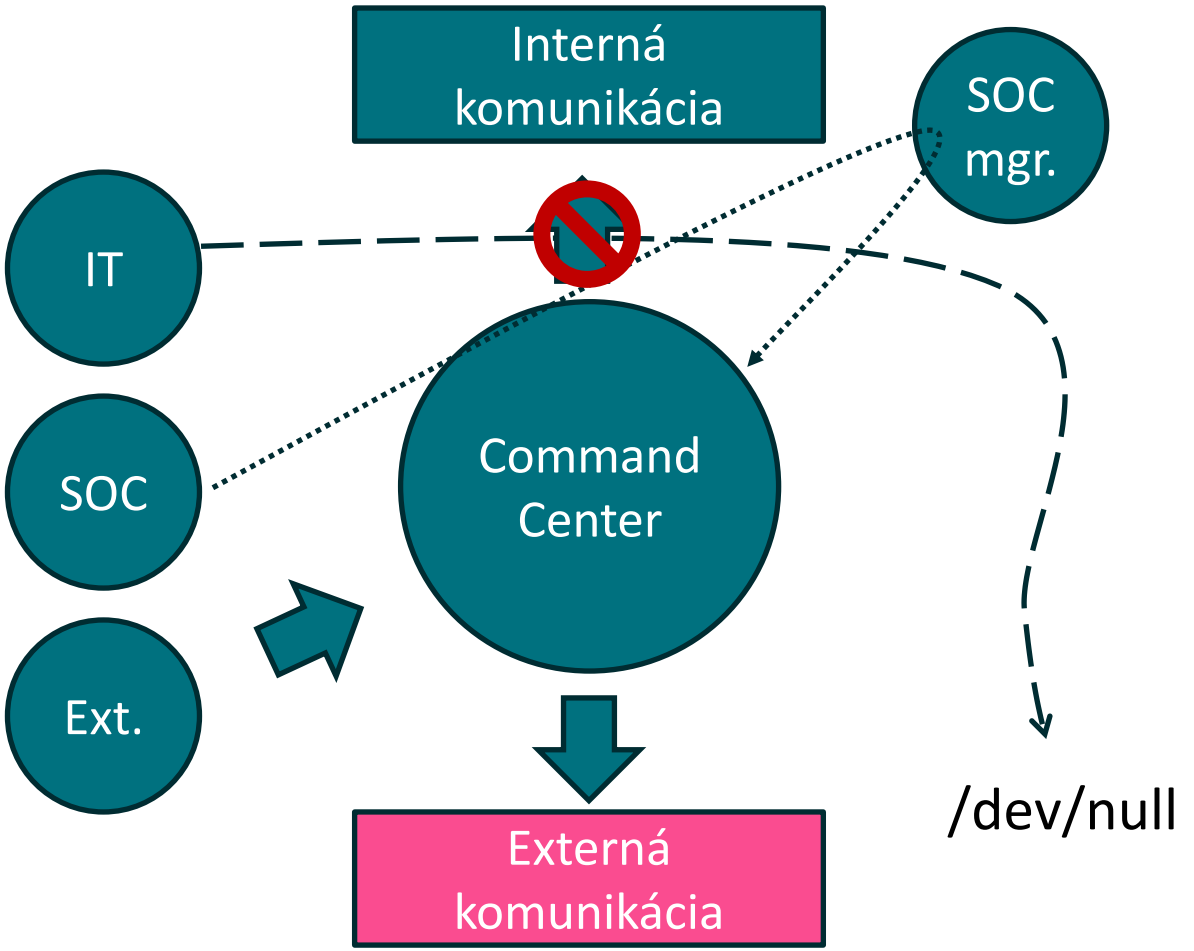
Hriech najväčší: nekomunikovanie
...alebo incident riešime, akurát sme vám to zabudli povedať

Sources:
https://www.bbc.co.uk/news/technology-41347467
https://www.bizjournals.com/orlando/news/2017/09/10/equifax-gets-blasted-for-cybersecurity-hack-on.html

Equifax offered no further comment beyond the materials they had published on an informational website.

Hriech najväčší: nekomunikovanie
...alebo incident riešime, akurát sme vám to zabudli povedať





Výsledok: Podať nesprávne informácie zlým spôsobom neskoro

Dlhá je cesta od riešiteľa k command centru

Možné problémy:

1. (nevie) Špecialista si rieši svoje
2. (nechce) Špecialista sa bojí povedať

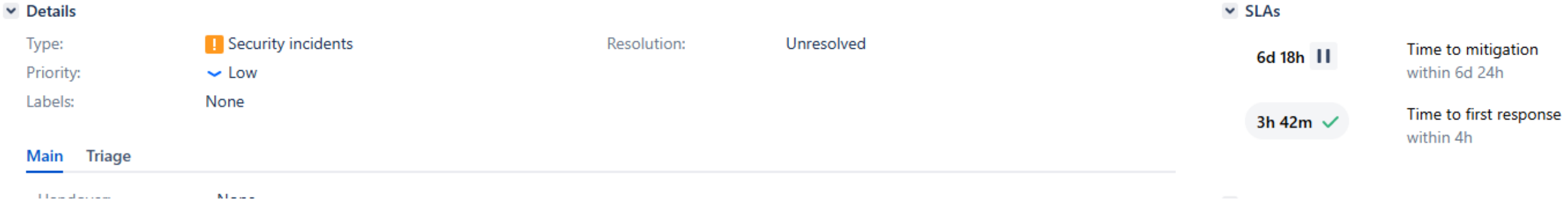
Riešenia:

- Procesy, jasná triáž – notifikačná matica
- Vzdelávanie, tréning, drill
- Dohľad nad IT incidentami
- Empatia

Tikajúce hodiny

Problém: povinnosti s jasným deadline na notifikáciu - NIS2, GDPR, zákazníci

SOC: Meráme? Meráme! MTTR, MTTM



Riešenie: tikajúce hodiny v IR toole

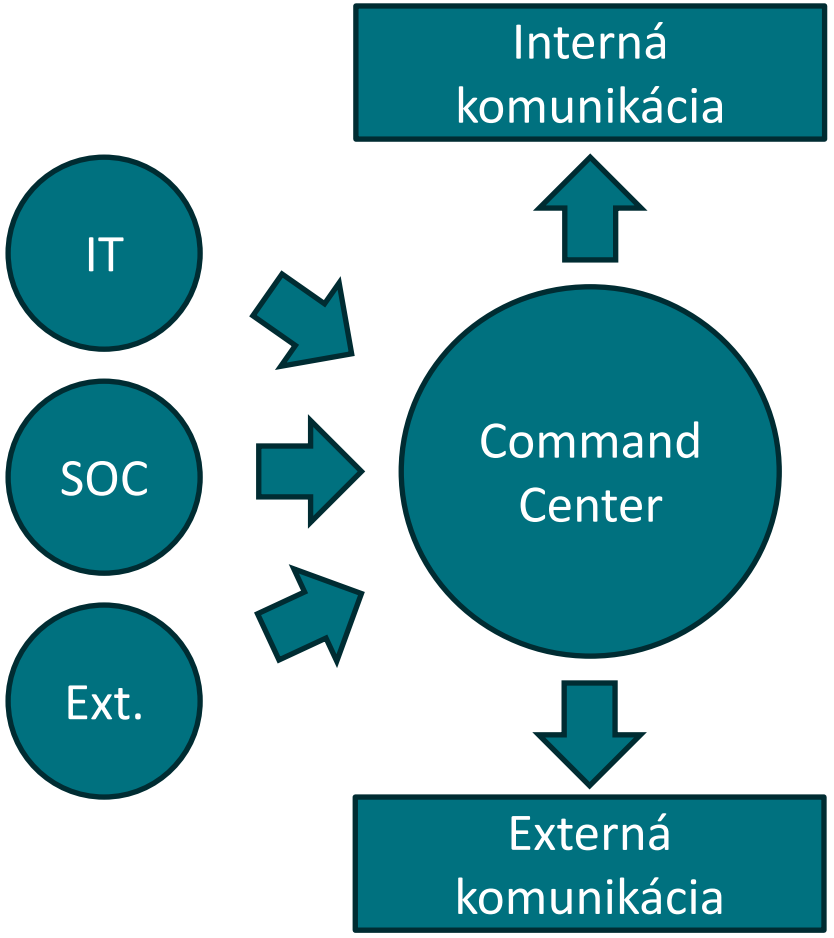
Stratení v komunikačných potrubiach
...alebo dáme vedieť PR a oni už komunikáciu vyriešia

Problém: Nevyriešia

Komunikácia na iných kanáloch? Partneri? Zamestnanci? Manažment?

Riešenie:

- Single source of truth
- Jasná autorizačná matica
- Jasná komunikačná matica – Kto? Komu? (do)Kedy?



Už tam budeme? Už tam budeme? Už tam budeme?

Pages / Internal Security Home / Meeting notes 1 Jira link Analytics Edit View inline comments Save for later Watching Share

20230928 libwebp vulnerability handling

Created by [redacted] last modified by [redacted]

Important status info:

- **Active phase of incident handling closed on** 09 Oct 2023 **. Switching to operative mode - hunting and patching vulns in infrastructure.**
- **Rapid7 signature released for packages - scanning possible, but only on package level (no scanning of lib itself)**
- **Firefox patches - ready**
- **Chrome patches - ready**
- **no info on internally developed applications / products being affected, suspicions:**
  - [redacted] **- analysis in progress**
  - [redacted] **analysis in progress**
- [redacted] **→ in security monitoring**

Open tasks and deadlines:

- [x] [redacted] dump list of SW installed from [redacted] - 29 Sep 2023 - first prioritize
- [x] [redacted] - check if possible to block webp on WAF
- [x] [redacted] send Dano info on forbidden SW - what? where (hostname)? who (owner from description)?
- [x] [redacted] check SaaS cloud vendors advisories
- [x] [redacted] - send powershell to Erik to identify owners from computer names
- [ ] *Click to add a new task...*

Patch level info:

Application patches

Application	Patching status	R7	SCCM	Forbidden	Description
[redacted]	IN PROGRESS	2734	2861	False	[redacted]
[redacted]	IN PROGRESS	2754	2822	False	
[redacted]	IN PROGRESS	3269	3353	False	

Meeting minutes:

09 Oct 2023 9:30

- infrasturcture patching:
  - SaaS advisories - [redacted] will check
  - Skype - mass uninstall in D598 - [redacted] will escalate i MS team
- inhouse developed apps (products / SaaS clouds / internal tools):
  - suspicious: report printer in [redacted]
  - suspicious: File open dialog vulnerable ? **REJECTED**
  - siter lib for GUI - to review
  - no report came from Dev teams

04 Oct 2023 11:30

- infrasturcture patching:
  - SaaS advisories - [redacted] will check
  - Skype - mass uninstall in D598 - [redacted] will escalate i MS team
- inhouse developed apps (products / SaaS clouds / internal tools):
  - suspicious: report printer [redacted]
  - suspicious: File open dialog vulnerable ?
  - no report came from Dev teams

02 Oct 2023 8:30

- Communication:
  - no communication to incident@eset.com so far
  - **if anything found in ESET products / apps notify** [redacted]
- infrasturcture patching - [redacted] will cover till
  - packages via [redacted] pushed to servers

Riešenia

1. Dokumentácia – jasná triage a notifikačná autorizačná a komunikačná matica
2. Dokumentácia – single source of truth, komunikačná matica
3. Podpora nástrojov – tikajúceho hodiny, vizibilita
4. Tréning, drilovanie
5. **Empatia**

SECURITY DAYS

Ďakujem za pozornosť

Digital Security
Progress. Protected. & SME KONFERENCIE