

Bezpečnost dodavatelů v oblasti OT

-

poznámky k možnostem × realitě

Jiří Kasner, kasner.jiri@colaut.cz

COLSYS
AUTOMATIK



HIRSCHMANN

A **BELDEN** BRAND

Přehled základních témat...

- Obvyklý stav věci (pohled do historie a pohled do současnosti).
- Smluvní dokumentace (co je vlastně cílem).
- Bezpečnostní cyklus u dodavatele z pohledu objednatele.
- Jaká jsou problematická místa, proč jsou problematická a jak s nimi naložit.
- V jakém stavu je vlastně vztah odběratele a dodavatele.
- Klíčový dodavatel a náležitá obchodně – politická obsluha vztahů.

Obvyklý stav věci.

- Otázky typu:
 - Kdo nám to vlastně dodává?
 - Máme s ním vůbec nějakou smlouvu?
 - Toho jsem tu už rok neviděl...
 - A podobně.
- Velké problémy s identifikací rozsahu znalostí vlastních a dodavatelských.
- Telefonista a přeposílač mailů? ☹️
- V čem je vlastně dodavatel kritický?
- Proč ty dodavatelské vztahy vlastně řídit? Všechno nám funguje... Vážně?
- Co vlastně dodavatel zajišťuje z pohledu obnovení provozu po nějakém incidentu?

Smluvní dokumentace.

- Co to vůbec je?
- K čemu je taková dokumentace dobrá z pohledu řízení rizik?
- Vazby a protiplnění ze strany objednatele.
- Úzká hrdla spolupráce.
- Dlouhodobé × krátkodobé smlouvy – jak na to a proč.
- Vendor lock?

Bezpečnostní cyklus.



- Argumentace u klíčových dodavatelů stran bezpečnostního cyklu.
 - Někdy je problém, že dodavatelům se „nechce“.
- Audity a cyklické debaty s dodavateli?
- Co s výsledky auditu a jak s nimi pracovat (politicko – obchodní práce).
- Co vlastně je zajímavé sledovat a hodnotit u dodavatelů – na co si dát pozor.
- Existují různé metody sledování stavu dodavatelů a často jsou tak levné, že jejich nepoužívání vůbec nedává smysl...
- Je dobré se dívat na tento proces i z druhé strany – zametení vlastní zahrádky...

Jaká jsou problematická místa, proč jsou problematická a jak s nimi naložit.

V jakém stavu je vlastně vztah odběratele a dodavatele.

Klíčový dodavatel a náležitá obchodně – politická obsluha vztahů.

- Obecně platí, že v každém obchodním vztahu existují místa, která je potřeba mít ošetřená.
- Je dobré si uvědomit, že bezpečnost je stále přirozenou součástí vztahů.
- Ošetřená místa jsou typicky ta, kde cítíme riziko nebo problém:
 - riziko incidentu z vnitřku nebo z vnějšku (nefunkčnost, nedostupnost, ...) – SLA, pohotovost apod.,
 - riziko poruchy technologie – testy, kontroly, revize apod.,
 - problém se stabilitou dodavatele – audit, sledování dodavatele,
 - a další.
- Je velmi moudré, aby společně s daným aktivem byl jeho dodavatel vnímán jako riziko a takto se k němu přistupovalo – ten vztah je o zdravém hodnocení rizika mezi 2 subjekty.
- U klíčových dodavatelů je postup ještě důležitější – včetně mapy vztahů a posouzení ekonomických, obchodních a dalších rizik pro případ zhoršení nebo zhroucení vztahů (soft skills a to je občas problém).