Void

Security Operations Center

Void

One service.
Zero worries.

Security Operations Center

- 24/7 aktívny dohľad nad kybernetickou bezpečnosťou
- založené na štandardoch a best practice NIST, TI, ENISA...
- poskytované formou služby
- súčasť medzinárodnej komunity združujúcej CSIRT/SOC tímy

VOID SOC
Accredited
since 01 Nov 2019

ACCREDITED BY TRUSTED INTRODUCER
TI

Void
One service.
Zero worries.

Výskum - metóda

1. Zameranie výskumu na ICS
2. Tím analytikov kybernetickej bezpečnosti Void SOC
3. Práca s verejne dostupnými dátami a systémami na internete
   - read-only prístup
   - žiaden “hacking“
   - žiadne hádanie hesiel, žiadne prihlasovanie
   - žiadne zmeny v systémoch
4. Realizovaný počas leta 2019

Void
One service.
Zero worries.

Výskum – vzorka

1. ICS na území SR, dostupné z internetu
2. ICS rôznych výrobcov

   Siemens, ABB, Schneider Electric, Honeywell, Johnson Controls, Rockwell Automation a ďalší...

Void
One service.
Zero worries.

Výskum - zistenia

1. 509 ICS systémov prístupných cez internet
2. Často ignorujú základné bezpečnostné odporúčania
3. Otvorené pre anonymný prístup pre kohokoľvek
4. Bežne používané staré verzie (napr. z 2007)
5. Celoslovenský problém – ICS lokalizované v 114 mestách

*Identifikovateľné subjekty tím VoidSOC upozornil na slabé zabezpečenie a hrozby.

Void
One service.
Zero worries.

Prečo je to problém?

1. ICS verejne prístupný z internetu priťahuje útočníkov aj malware
2. Neaktuálne verzie softvéru majú známe „diery“ ktoré sa dajú zneužiť
3. Zneužitý systém môže škodiť alebo slúžiť ako prestupná stanica
4. Takýto stav môže znamenať slabé zabezpečenie celej firmy
5. Priemerná doba odhalenia prieniku je 214 dní

Void
One service.
Zero worries.

Ukážka 1 - verejne dostupný ICS v mraziarňach

Gastra

SENSORS

Sensors

	Name	Safe Range	Hysteresis	Delay [s]	SNMP Trap	Email	SMS
Sensor ID: 24629 Code: 28603585050000e6 Value: **-19.8 °C**	Sklad G14	10.0 .. 60.0	0.0	0	☐	☐	☐
Sensor ID: 29204 Code: 28721485050000e6 Value: **-18.3 °C**	Sklad G12	10.0 .. 60.0	0.0	0	☐	☐	☐
Sensor ID: 33669 Code: 28838585050000d9 Value: **-26.2 °C**	Sklad G5	10.0 .. 60.0	0.0	0	☐	☐	☐
Sensor ID: 45545 Code: 28b1e984050000e5 Value: **-18.4 °C**	Sklad G13	10.0 .. 60.0	0.0	0	☐	☐	☐
Sensor ID: 49685 Code: 28c215850500002c Value: **-21.0 °C**	Sklad G6	10.0 .. 60.0	0.0	0	☐	☐	☐
Sensor ID: 61833 Code: 28f189850500000e Value: **-22.9 °C**	Sklad G11	10.0 .. 60.0	0.0	0	☐	☐	☐

Void
One service.
Zero worries.

Ukážka 2 - verejne dostupný ICS vo vodnej elektrárni

Void
Security Operations Center

12:17:37 PM

Void
Security Operations Center

Výkon MVE	[redacted]
Horná hladina	166.109 m
Dolná hladina	161.356 m

	TG1	TG2
Režim riadenia	AUT	AUT
Stav	TURB	TURB
Typ. regulácie	HL. REG	OPT. VYK
Súborný alarm	VYS POR	VYS POR
Výkon	[redacted]	[redacted]
Poloha RK	50 %	54 %
Poloha OK	25 %	33 %

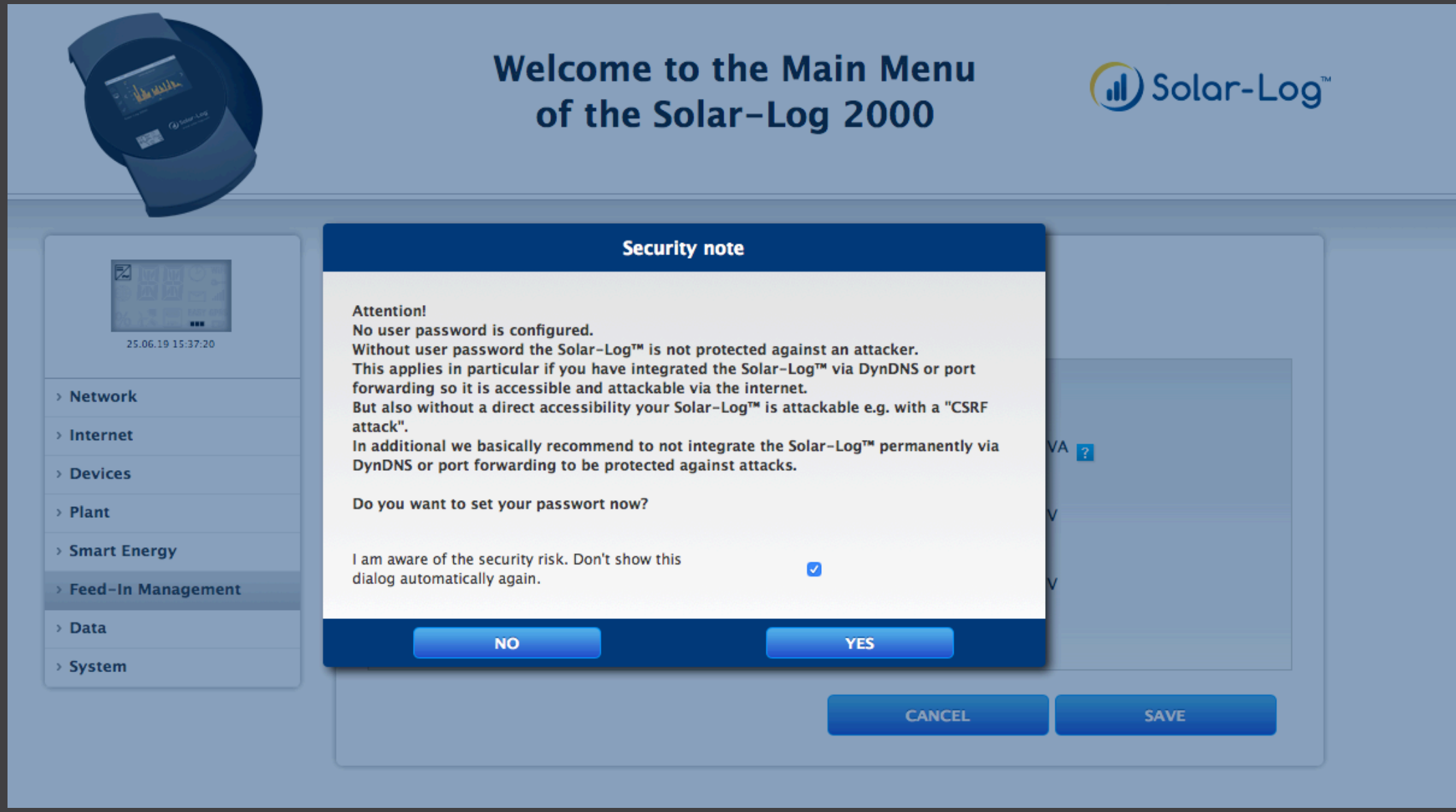
Stav MVE | Záznamy | SMS | Alarmy | ???

Void
One service.
Zero worries.

Ukážka 3 - verejne dostupný ICS monitorujúci kvalitu odpadových vôd

Void
One service.
Zero worries.

Ukážka 4 - verejne dostupný ICS fotovoltaickej elektrárne



Void
One service.
Zero worries.

Prečo nie sú firmy „safe“

- Dlhý životný cyklus technológií používaných vo výrobe
- Postupná „digitalizácia“ a „automatizácia“ – premena starších rozmanitých technológií na štandardizované
- Zraniteľné zariadenia a systémy riadia veľkú časť výroby a majú dosah na bezpečnosť výroby
- Do kybernetickej bezpečnosti sa neinvestovalo priebežne

Void
One service.
Zero worries.

Ako byť viac „safe“

- Implementácia bezpečnostných riešení,
- Budovať povedomie o kybernetickej bezpečnosti
- Zaviesť podnikovú bezpečnostnú stratégiu, best practices, príp. certifikáciu
- Proaktívne monitorovať vlastné prostredie
- Pripraviť sa na kritické situácie a potom správne reagovať
- Proaktívne a priebežne riešiť novovznikajúce riziká a kritické miesta

Void

One service.
Zero worries.

Ďakujem za pozornosť_

mlohnert@voidsoc.com