Řešení fyzické a kybernetické bezpečnosti v oblasti IT a non-IT

Jan Kašpar, Schneider Electric

+420 739 891 841
jan.kaspar@se.com

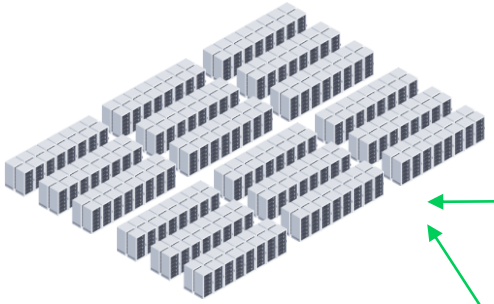
Agenda

1. Kompletní infrastruktura – IT, non-IT, OT
2. Požadavky na zabezpečení - vyhláška
3. Řešení přístupu a dohledu prostředí
4. Kybernetická bezpečnost pro non-IT
5. Dostupnost infrastruktury - doporučení

Life Is On Schneider Electric

Architektura IT současné doby – hybridní model

Centralizované DC



CENTRALIZOVANÁ

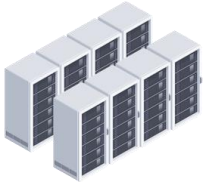
Obrovský výpočetní výkon
a kapacita ve vzdálené lokalitě

Prodejní místa

LOKÁLNÍ EDGE

Výpočetní výkon a kapacita
v místě kde se data vytváří
– okraj sítě

Regionální kanceláře



REGIONÁLNÍ EDGE

Vysoký výpočetní výkon a kapacita
v místní lokalitě

Očekávání zákazníků

DOSTUPNOST

62%

Výpadků IT služeb a infrastruktury lze přičíst selhání infrastruktury ze strany dodavatelů cloudu a kolokačních operátorů

(Zdroj: Uptime Institute)

BEZPEČNOST

#1

V seznamu rizik podle Allianz Risk Barometer 2022

(Zdroj: Allianz)

EFEKTIVITA

99%

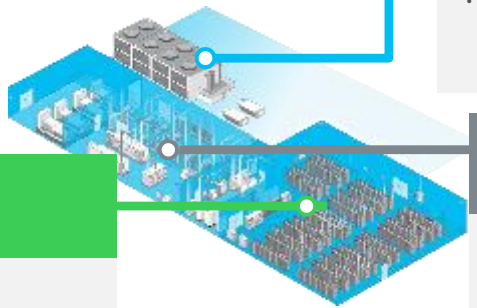
Vedoucích představitelů velkých společností souhlasí, že efektivita a udržitelnost je kritická pro jejich budoucí podnikání

(Source: Harvard Business Review)

Life Is On Schneider Electric

Navzájem propojená infrastruktura a její bezpečnost

Příklad kompletního prostředí – fyzická infrastruktura a dohledové nástroje



Technologie :

- Venkovní chladící jednotky
- Výměníky vzduchu
- Odvody tepla, čerpadla
- Požární a bezpečnostní systémy

EcoStruxure Building Advisor

Napájení :

- UPS
- Distribuce elektřiny
- Rozvaděče (MV, LV)
- Přípojnicové systémy
- Měření spotřeby a sensory
- Jističe
- Transformátory

EcoStruxure Power Advisor

EcoStruxure IT Advisor

Části fyzické infrastruktury IT :

- Napájení
- Distribuce el. energie (PDU / ATS)
- Chlazení
- Monitoring prostředí
- Přístupové systémy
- a další podobné v této kategorii

a v některých případech také :

- Servery
- Disková pole
- Datovou síť

Life Is On Schneider Electric

Vyhláška č. 82/2018 Sb. (vyhláška o kybernetické bezpečnosti)

HLAVA I

§ 12 **Řízení přístupu**
§ 14 Zvládání kybernetických bezpečnostních událostí a incidentů
§ 15 Řízení kontinuity činností
§ 16 **Audit kybernetické bezpečnosti**
§ 21 **Ochrana před škodlivým kódem**
(1) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona v rámci ochrany před škodlivým kódem
a) s ohledem na důležitost aktiv zajišťuje **použití nástroje pro nepřetržitou automatickou ochranu**
5. komunikační sítě a prvků komunikační sítě a
6. obdobných zařízení,

§ 28 **Průmyslové, řídicí a obdobné specifické systémy**
b) **omezení fyzického přístupu** k zařízením těchto systémů a ke komunikační síti,
e) **ochranu jednotlivých technických aktiv** těchto systémů před **využitím známých zranitelností**

HLAVA II § 17 **TECHNICKÁ OPATŘENÍ**

Fyzická bezpečnost, povinná osoba v rámci fyzické bezpečnosti
a) **předchází poškození**, krádeži nebo **zneužití aktiv nebo přerušení poskytování služeb** informačního a komunikačního systému,
c) u fyzického bezpečnostního perimetru stanoveného podle písmene b) přijme nezbytná opatření a **uplatňuje prostředky fyzické bezpečnosti**

Výše uvedené jsou pouze vybrané části vyhlášky relevantní pro tuto prezentaci

Možnosti financování : Kybernetická bezpečnost – IROP II

IROP 2021-2027 > eGovernment a kyberbezpečnost

EQUICA

Home | Naše služby | O nás | Reference | Blog | Kontakt | POPTÁVKOVÝ FORMULÁŘ

Oprávnění žadatelé – předpoklad

- Organizační složky státu, příspěvkové organizace organizačních složek státu, státní organizace, státní podniky, kraje, organizace zřizované nebo zakládané kraji, obce, organizace zřizované nebo zakládané obcemi.

Na co lze získat dotaci (předpoklad)?

- Projekty oprávněných žadatelů, v rámci nichž oprávnění žadatelé zabezpečují **kritickou informační infrastrukturu, významné informační systémy nebo informační systémy základních služeb**, které sami spravují, či které spravuje oprávněnému žadateli podřízená a jím ovládaná organizace, která je taktéž oprávněným žadatelem.
- Podpora **ostatních informačních a komunikačních systémů**, které nespadají pod výše uvedené a které oprávněný žadatel sám spravuje nebo které spravuje oprávněnému žadateli podřízená a jím ovládaná organizace, která je taktéž oprávněným žadatelem.
- Podporovány budou aktivity naplňující **technická opatření** dle vyhlášky o kybernetické bezpečnosti:
  - Fyzická bezpečnost
  - Nástroj pro ochranu integrity komunikačních sítí
  - Nástroj pro ověřování identity uživatelů
  - Nástroj pro řízení přístupových oprávnění
  - Nástroj pro ochranu před škodlivým kódem
  - Nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
  - Nástroj pro detekci kybernetických bezpečnostních událostí
  - Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
  - Aplikační bezpečnost
  - Kryptografické prostředky
  - Nástroj pro zajišťování úrovně dostupnosti informací
  - Bezpečnost průmyslových a řídicích systémů

Směrnice NIS2

- Směrnice Evropského parlamentu a Rady Evropy o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Evropské unii
- Povinnost zavést organizační i **technická opatření** k zajištění ochrany jejich informačních systémů
- Publikace finálního znění na konci roku 2022
- Předpokládaná platnost (ČR) od poloviny roku 2024, prostřednictvím novely zákona o kybernetické bezpečnosti
- Výrazné rozšíření počtu povinných organizací a subjektů, ze stávajících několika-set organizací na **více jak 6 000** (základní a důležité organizace)

Nové sektory a subjekty:

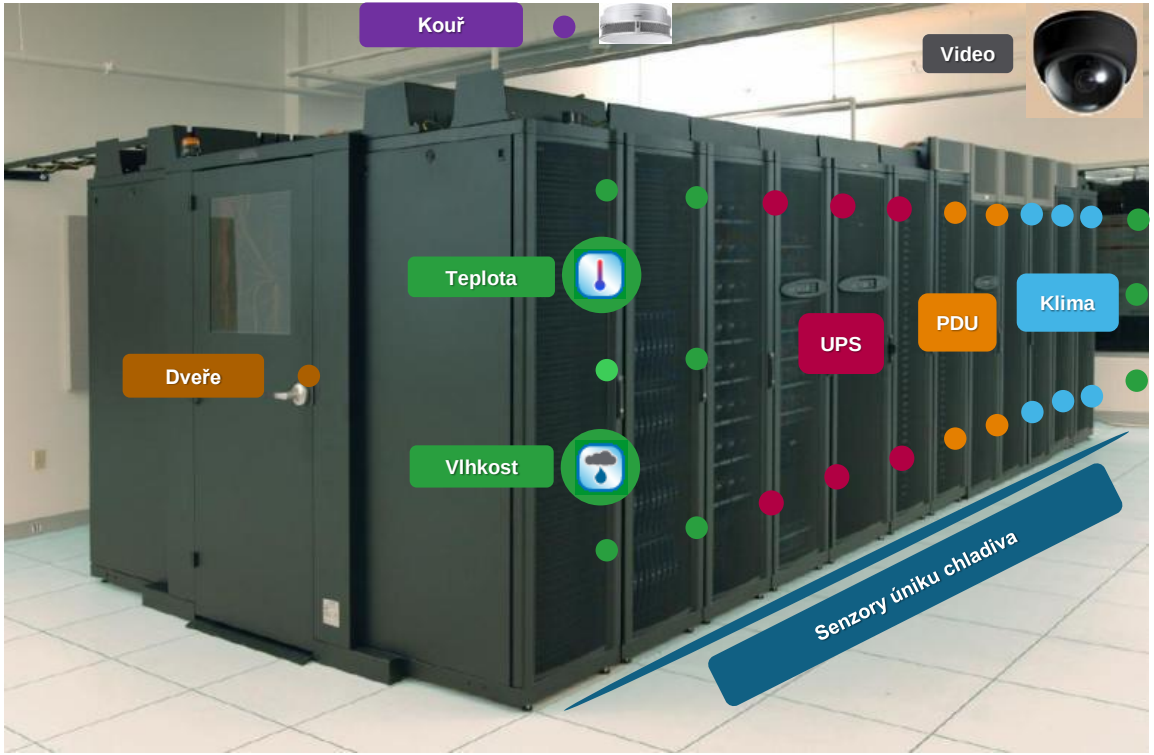
- Provozovatelé výroby, skladování a přepravy vodíku
- Zdravotnictví – rozšíření o referenční laboratoře
- Cloudy, on-line tržiště, vyhledávače – nový režim
- Datová centra, sociální sítě
- Content delivery network providers
- Poskytovatelé služeb vytvářejících důvěru
- Sítě a služby el. komunikací – nový režim
- Managed service providers (MSP), Managed security service providers (MSSP)
- Veřejná správa (centrální, regionální)
- Vesmír
- Poštovní a kurýrní služby
- Odpadové hospodářství
- Výroba a distribuce chemických látek
- Výroba a distribuce potravin
- Výroba vybraných zařízení a prostředků
- Dobíjecí stanice elektroaut
- Výzkumné instituce

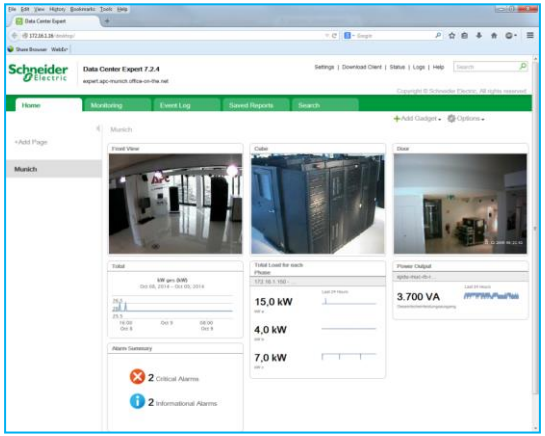
Obvyklé dotazy k dostupnosti a zabezpečení infrastruktury

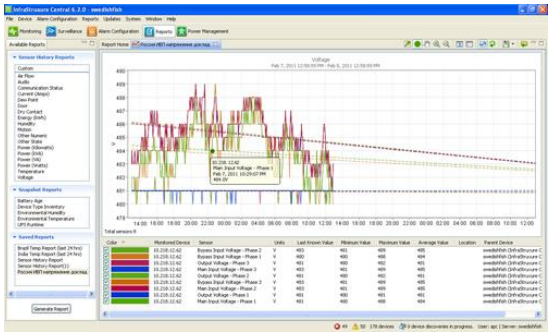
- Jakým způsobem proaktivně dohledujete vaši IT infrastrukturu ?
- V jakém počtu lokalit provozujete IT technologie, máte v těchto lokalitách technickou podporu ?
- Nastaly v předchozím období neočekávané a nežádoucí výpadky IT technologií z důvodu narušení provozního prostředí nebo nevyhovujícím podmínkám ?
- Dokážete vyčíslit dopad výpadku provozu IT infrastruktury na Váš provoz / podnikání ?
- Máte zabezpečený přístup k IT technologiím včetně evidence událostí ?
- Jakým způsobem máte nastavena pravidla pro řízení rizik a zodpovědnosti v rámci vaší organizace ?

Zajištění fyzické bezpečnosti a prostředí mimo serverovny

Monitoring fyzického prostředí a kontrola přístupu







Proč jsou důležité provozní podmínky a zabezpečení

Rizika spočívající v **provozním prostředí**		Rizika spočívající v oblasti **zabezpečení**
Teplota		Vyšší teplota zpravidla znamená nejen riziko výpadku, ale také kratší životnost provozovaných technologií nebo jejich horší efektivitu.
Vlhkost, nízká/vysoká		Nízká vlhkost s sebou přináší možnost elektrostatického výboje. Vysoká vlhkost představuje přímé nebezpečí pro IT zařízení.
Kapaliny/netěsnosti		Není překvapením, že voda neprospívá životnosti IT technologií a chladící systémy a potrubí nepatří do prostoru nad IT RACKy.
Kouř / požár		Důsledkem přehřátí jednoho zařízení může být kouř nebo požár, který ale nemůže ohrozit dostupnost služeb celé serverovny nebo datového centra.
Kontrola přístupu		Oblast ochrany informací, kdy je třeba splnit potřebná nařízení a zamezit ztrátě nebo zneužití informací. Ochrana zařízení a dat na úrovni RACKu je kriticky důležitá.
Dohled		Některé organizace potřebují uchovávat záznamy z kamerového systému po dobu přibližně 5 let, aby vyhověly předpisům.

Life Is On Schneider Electric

NetBotz - kompletní řešení,přístup a dohled fyzického prostředí

Kontrola přístupu, kamerový dohled, sensory a spínače, centrální správa a management

NetBotz se skládá ze zařízení pro montáž do racku a na stěnu navržených tak, aby poskytovaly širokou škálu integrovaného monitorování prostředí a dohledu pro citlivá zařízení.

Senzorové moduly, POE kamerové moduly a HID přístupové moduly do racku se připojují pomocí kabelů USB nebo Cat-5.

Senzory zahrnují bezdrátovou a kabelovou detekci teploty a vlhkosti, kouře, vibrací a kapalin.

Řízení přístupu do racku přizpůsobené prostředím Datových Center a EDGE poskytuje vstup na základě oprávnění a auditní záznam.

SNMP – automatická identifikace připojených zařízení Schneider Electric (UPS, PDU atd.)

NetBotz Rack Access Monitor 250

Kompletní řešení dohledu a přístupu pro 1 RACK skříň

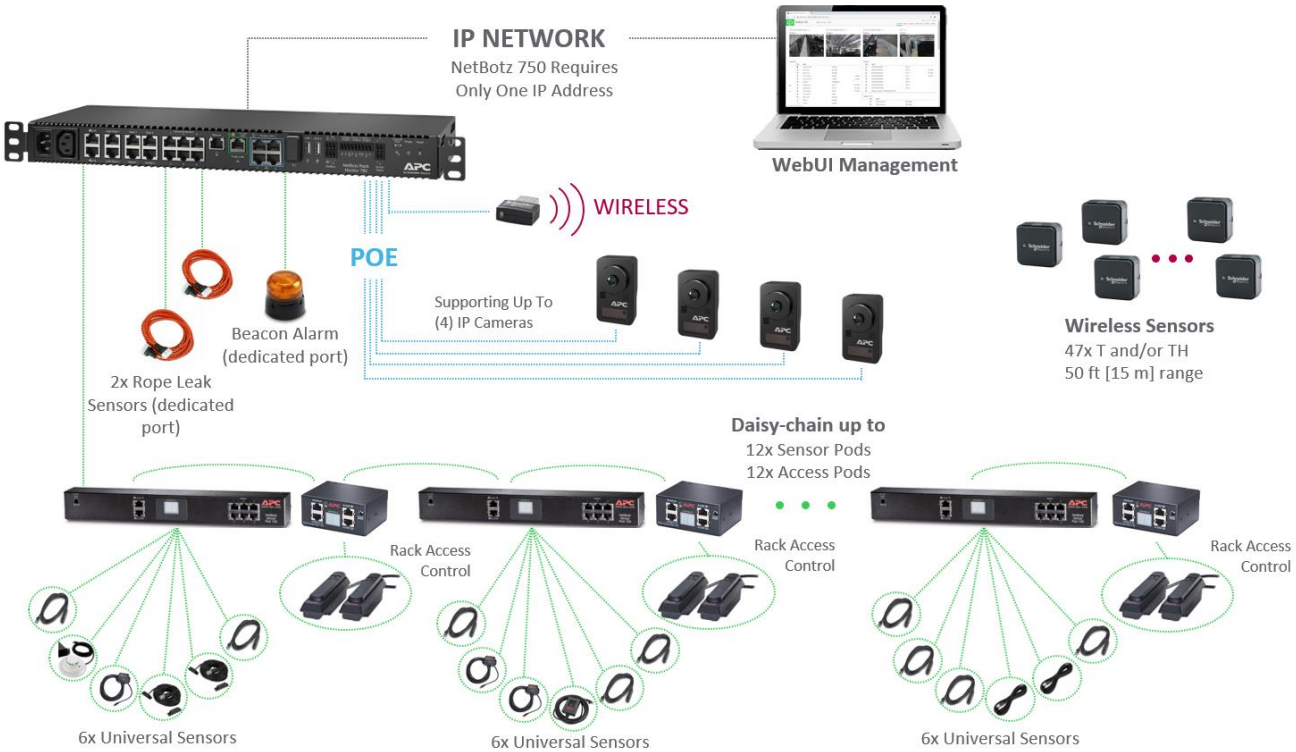
SKU NAME	NBACS125	NBACS1356
Description	Netbotz 250 appliance and rack access control solution with 125 kHz Handles	Netbotz 250 appliance and rack access control solution with 13.56 MHz Handles
Image		
Included	NetBotz 250 Appliance, wireless temperature sensor, wireless coordinator, wired temp/humidity sensor, (2) door contacts, (2) 125 kHz handle kits	NetBotz 250 Appliance, wireless temperature sensor, wireless coordinator, wired temp/humidity sensor, (2) door contacts, (2) 13.56 MHz handle kits
Supported cards	H10301 – Standard 26 Bit H10302 – 37 Bit w/o facility code H10304 – 37 bit w/ facility code CORP1000	MIFAREC4 – Mifare Classic 4 byte MIFAREC7 – Mifare Classic 7 byte MIFAREDF – Mifare DESfire MIFAREPL – Mifare Plus iClass

- Kompletní vybavení pro 1 RACK
- Real-time monitoring a řízení přístupu
- Více násobná kontrola přístupu
- Snadná a jednoduchá instalace
- Omezení kabeláže
- Možnost přesunu bezdrátových čidel podle potřeby
- Využití stávajících přístupových karet
- Správa : WEB UI, DataCenter Expert
- Autentikace lokální / RADIUS / RADIUS fail-over
- Pouze 1 x IP adresa na celé prostředí

Life Is On Schneider Electric

APC NetBotz 750

Kompletní řešení dohledu a přístupu pro serverovny a datová centra



Life Is On Schneider Electric

Další příklady nasazení Netbotz

Datová centra

Popis prostředí

Kontrolované a zabezpečené prostředí, obvykle v jedné lokalitě, non-IT technologie centrálně spravované cloud-based nebo on-premise dohledovými nástroji

Hlavní výhody řešení Netbotz pro zákazníka

Kamerový dohled, vysoké rozlišení při nízké světelnosti, duální vstupy pro sensory, bezdrátová čidla, správa přes webový prohlížeč

RACK skříně a malé serverovny

Popis prostředí

IT technologie umístěné v rámci jedné RACK skříně nebo na okraji EDGE infrastruktury, případně také ve více lokalitách, s potřebou zabezpečení a dohledu

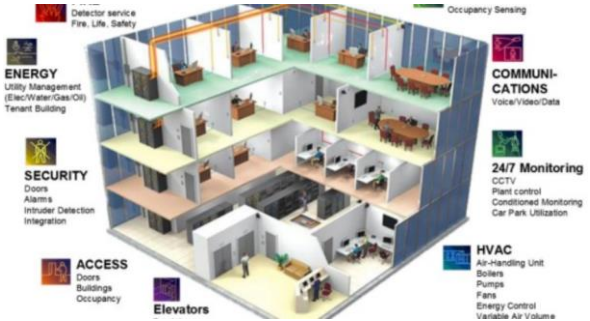
Hlavní výhody řešení Netbotz pro zákazníka

Kontrola přístupu, kamerový dohled, sensory a spínače, centrální správa a management, jedno kompletní řešení od rozsahu jedné RACK skříně nebo Mikro datového centra

Zabezpečení a správa budov

Popis prostředí

Stávající systém pro správu budovy (BMS) pro dohled a monitoring prostředí

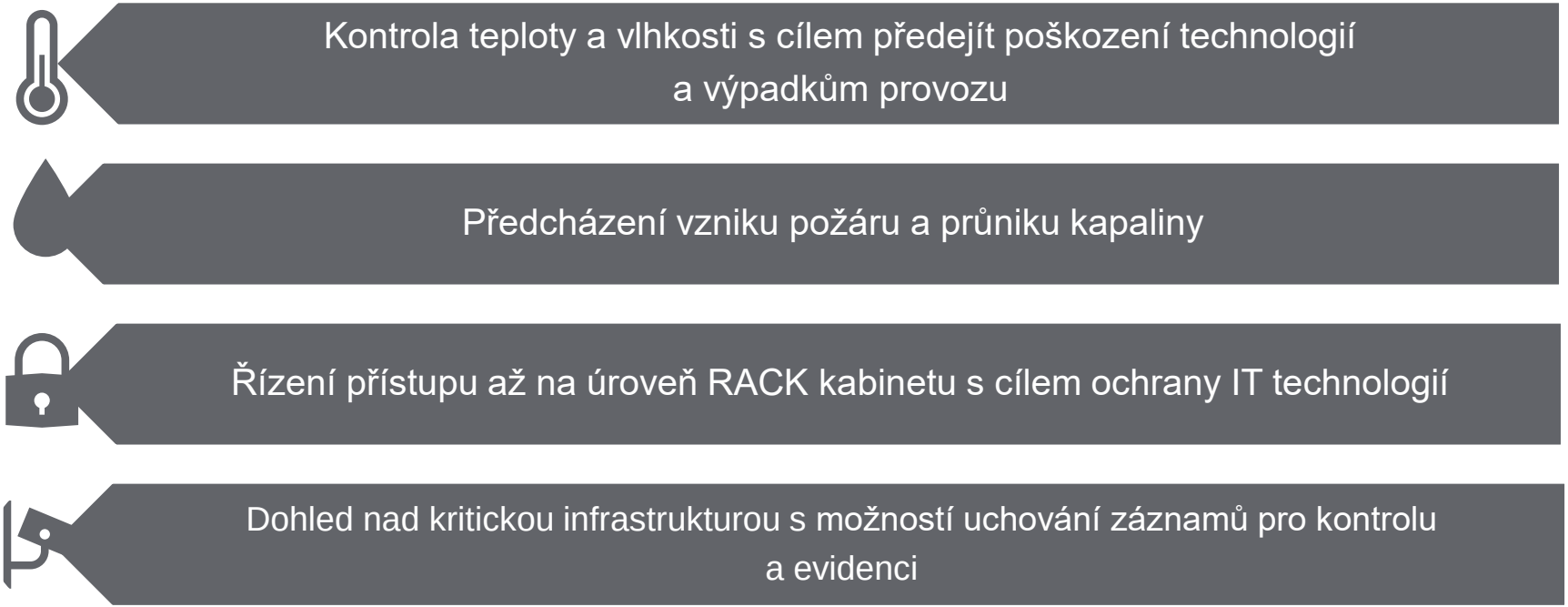


Hlavní výhody řešení Netbotz pro zákazníka

Plná integrace s BMS prostřednictvím protokolu Modbus, rozšíření možností stávajícícího systému řízení budovy prostřednictvím sensorů a kamer

Life Is On Schneider Electric

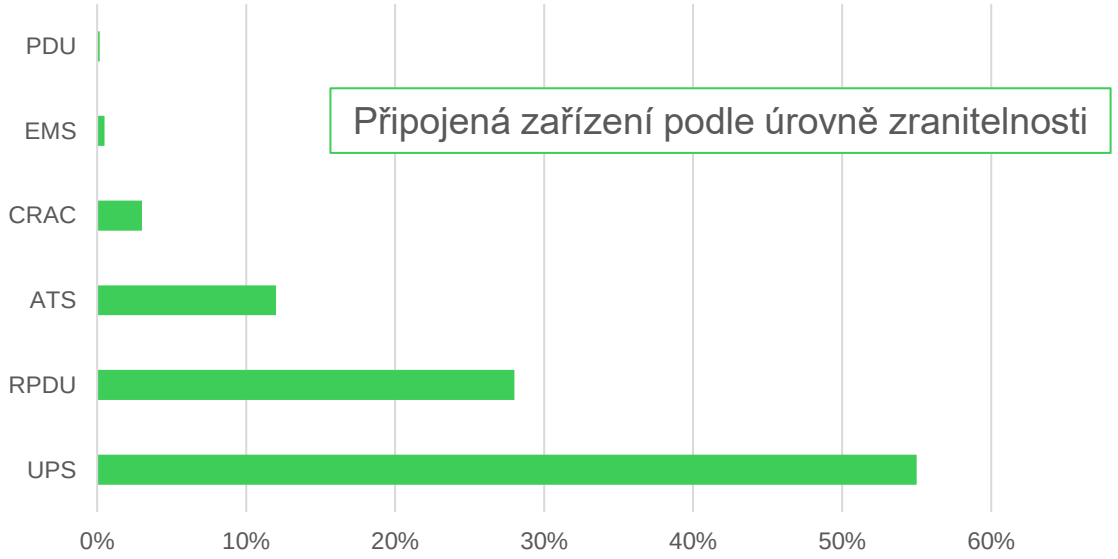
Hlavní výhody nasazení dohledu fyzického prostředí



Life Is On Schneider Electric

Kybernetická bezpečnost non-IT technologií

Všechna připojená zařízení představují potenciální zranitelnost celé infrastruktury



Source: EcoStruxure IT Data Lake

Life Is On Schneider Electric

Realita ...

62%

uživatelů provozuje zařízení s neaktuální verzí firmware a zvyšuje tak riziko zranitelnosti*

70%

zařízení která mají zranitelnost ji mají ve VŠECH těchto oblastech : File Transfer Vulnerability, Web Vulnerability, SNMP Access, Remote Access

*Kvalifikovaný odhad ze strany SE

Life Is On Schneider Electric

Hodnocení zranitelnosti připojených zařízení

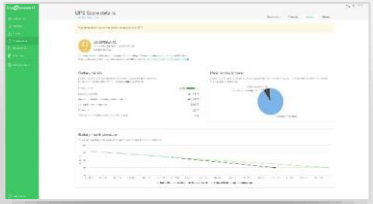
Snižte riziko narušení bezpečnosti

Life Is On Schneider Electric

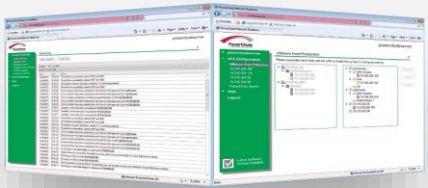
DCIM 3.0 – vyšší dostupnost, bezpečnost, efektivita

Snižte počet neplánovaných výpadků

Vyhodnocení stavu připojených zařízení



Plná integrace a proaktivní ochrana serverové a HCI infrastruktury

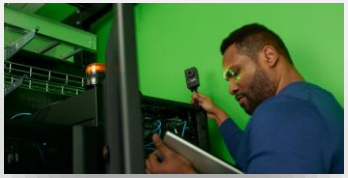


Testy pro odhlalení zranitelností

Měření celkové energetické efektivity až na úrovni připojených systémů, real-time PUE

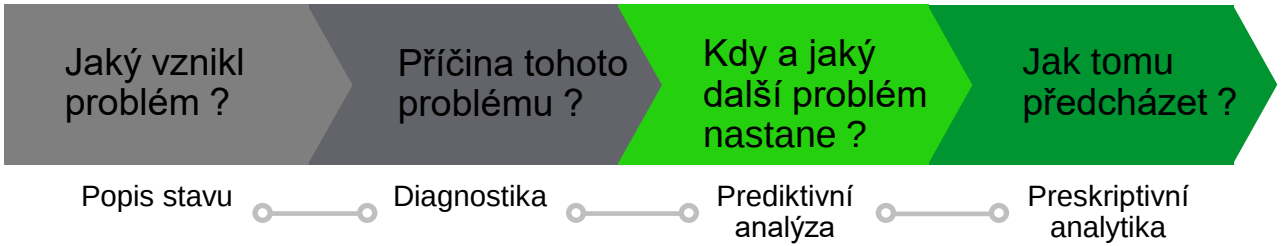
Monitoring fyzického prostředí s cílem předcházet výpadkům služeb a poškození IT technologií

Video záznamy a evidence přistupu pro účely kontroly a auditu, kontrola přístupu



Life Is On Schneider Electric

Nové možnosti dohledových nástrojů v cloudu



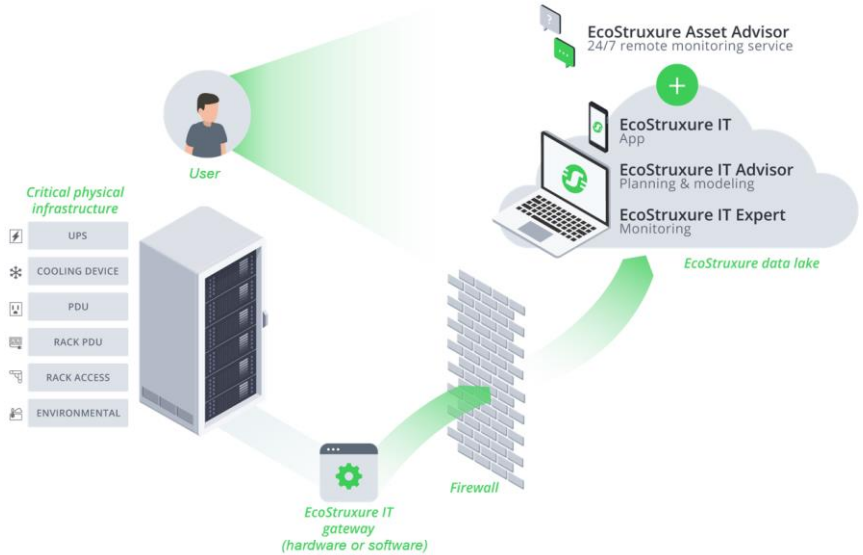
Možnosti nové generace cloud-based dohledových nástrojů

Tradiční on-premise dohledové nástroje

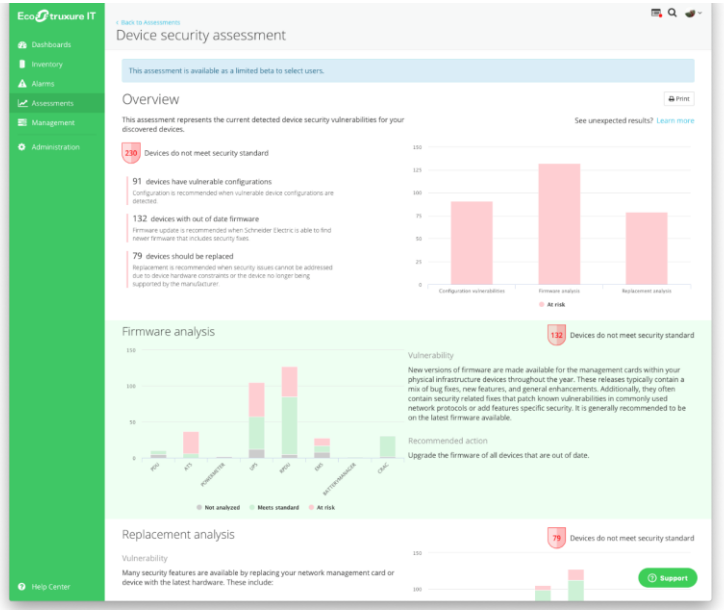
Life Is On Schneider Electric

EcoStruxure IT Expert – architektura řešení

- Dohledový nástroj nové generace, využívající cloud platformu MS Azure
- Kompletní pokrytí všech technologií z oblasti non-IT
- Výhody konceptu big data, umělé inteligence a prediktivní analýzy
- Otevřenost dalším výrobcům, API - možnost integrace s primárním dohledem



Kontrola a vyhodnocení zranitelností



- Doporučené změny včetně následného postupu
- Tisk souhrnné zprávy
- Export seznamu zranitelností do CSV souboru

Kontrola nastavení zařízení - konfigurací

Přehled neaktuálních a nezabezpečených konfigurací

Příklady doporučených změn komunikačních protokolů

- SNMP v3 vs. SNMP v1
- HTTPS vs. HTTP
- SSH vs. Telnet

Firmware

Informace o nových aktualizacích zabezpečení přímo pro Vaše připojená zařízení; cíl je okamžitá instalace bezpečnostnch oprav, jakmile jsou dostupné

Zařízení se zranitelnostmi

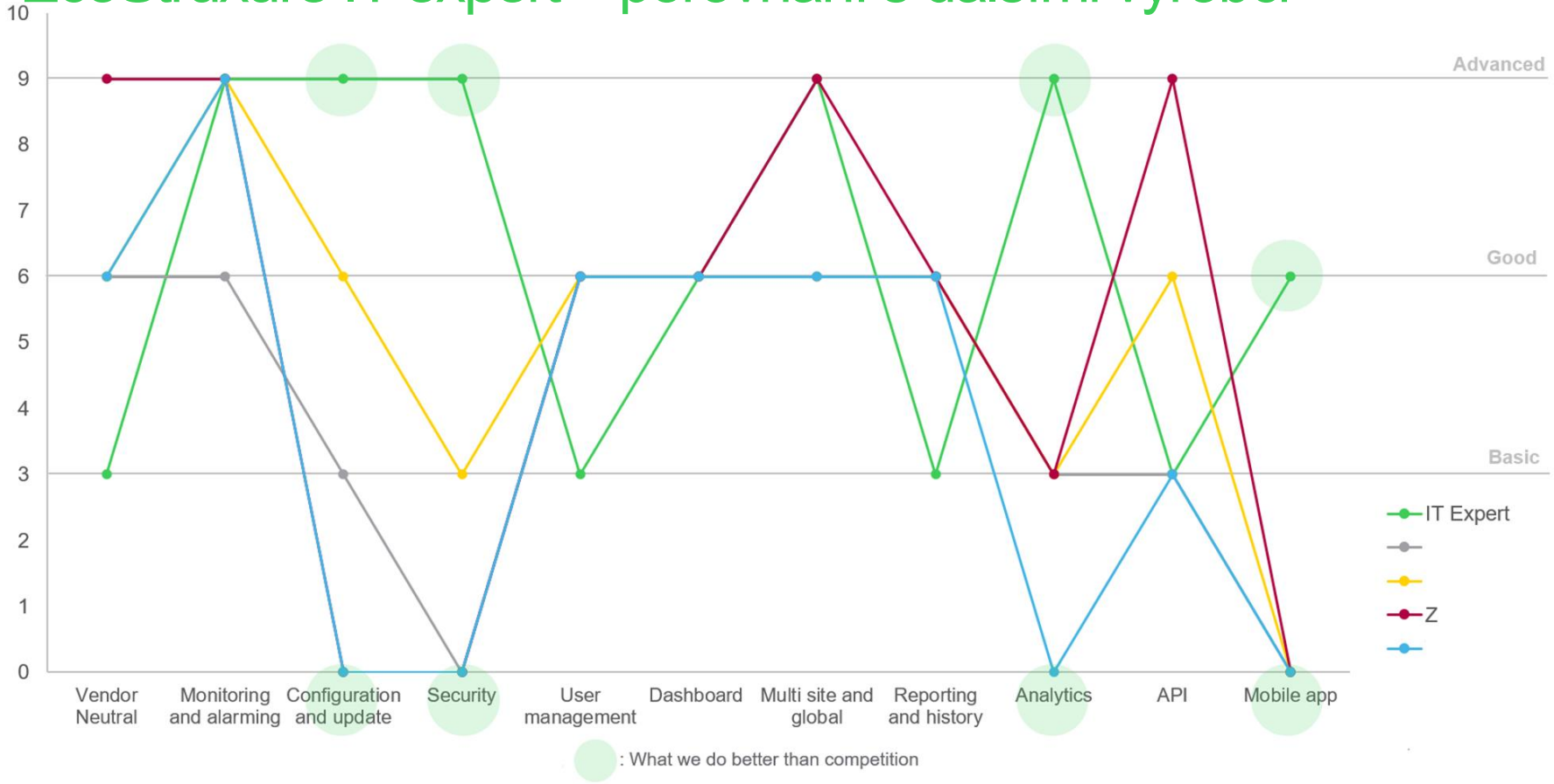
Identifikace zařízení, která neplní bezpečnostní standardy

Příklady

- Podpora TLS 1.2 a kontrola nastavení protokolu TLS 1.2
- Sledování a správa neoprávněného přístupu
- Deaktivace možnosti Pingu
- Možnost úpravy nastavení firewallu
- Správa uživatelských úrovní
- Správa přístupových oprávnění / hesel

Některé funkce jsou dostupné pouze pro produkty APC

EcoStruxure IT expert – porovnání s dalšími výrobci



Provoz IT technologií v rámci EDGE – **DOSTUPNOST**

Výzvy	Řešení	Příklady nových technologií
Životnost provozovaných technologií Prostředí s vyšší teplotou a prašností	Výběr produktů podle plánované životnosti Zajištění chlazení a použití prachových filtrů	Li-Ion v UPS
Fyzická bezpečnost (mimo serverovny) Kontrola přístupu k IT technologiím Evidence a dohled	Vytvoření prostředí pro provoz IT technologií Přístupový systém a úrovně oprávění Dohled včetně evidence	Mikro DC Centralizovaná správa přístupu a monitoring (NetBotz)
Kybernetická bezpečnost pro non-IT Aktualizace konfigurací a firmware Kontrola zabezpečení infrastruktury	Jeden dohledový nástroj pro kompletní non-IT Automatizace procesů, řešení vzdáleně a centrálně Detailní report úrovně zabezpečení	EcoStruxure IT
Provozní náklady (OPEX) Četnost prohlídek a oprav na místě Efektivita - spotřeba el. energie	Výběr produktů s nižší servisní náročností Technologie s nižší spotřebou el. energie – účinnost Dohledový nástroj – snížení počtu zásahů na místě	Li-Ion v UPS Přesné chlazení 50% úspora el. energie ECOnversion účinnost UPS 99%

Life Is On | Schneider Electric

Jan Kašpar
Managed Partner Account Manager
jan.kaspar@se.com
+420 739 891 841