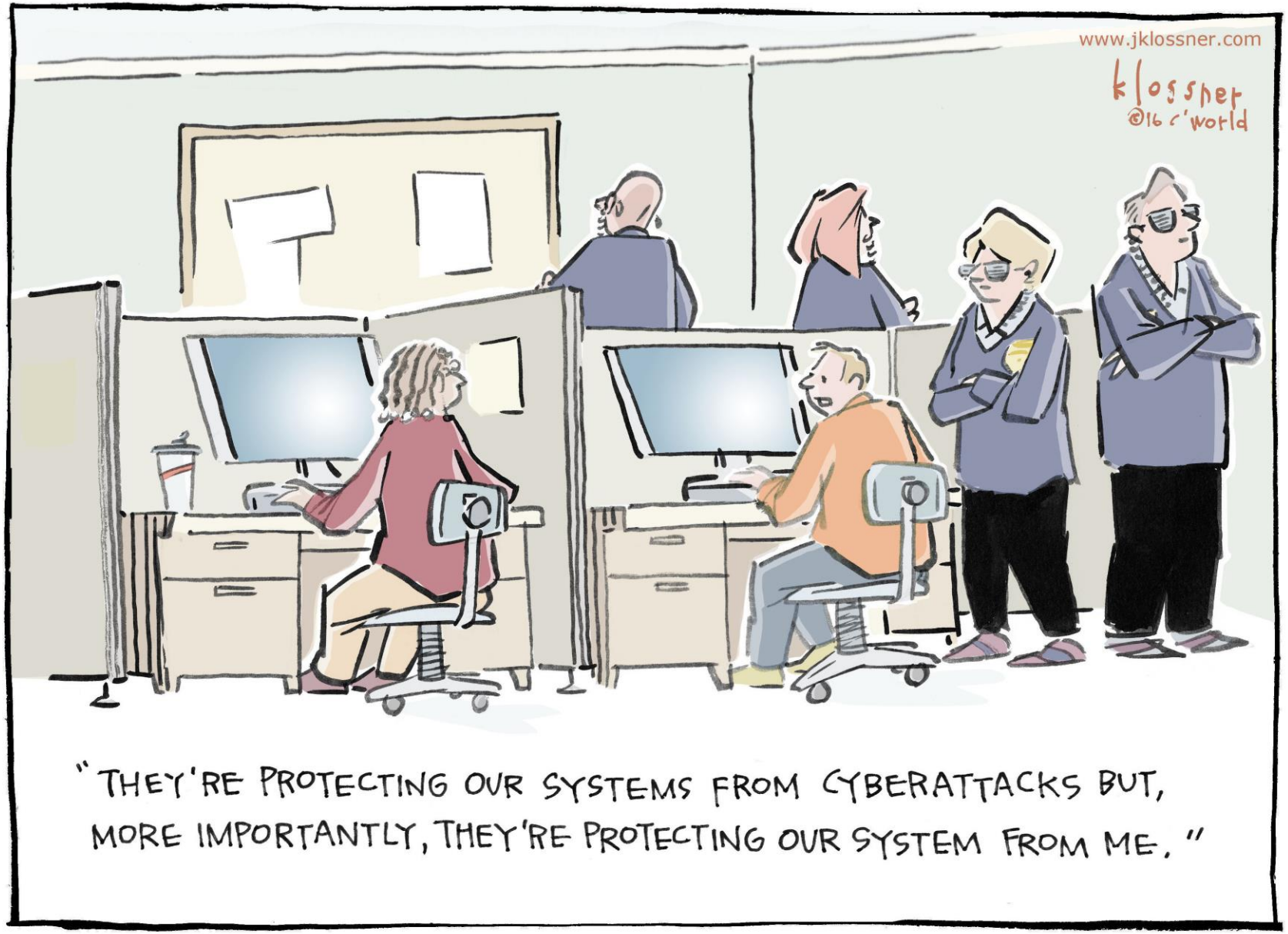

www.jklossner.com
klossner
©16 c'world
"THEY'RE PROTECTING OUR SYSTEMS FROM CYBERATTACKS BUT, MORE IMPORTANTLY, THEY'RE PROTECTING OUR SYSTEM FROM ME."

SODAT

SODAT

Jak se ztrácí citlivá data a jak tato data ochránit?:

Praktické zkušenosti a řešení incidentů

Jan Kozák

Senior Product Specialist

O NÁS

VÍCE JAK 20 LET NA TRHU

MÁME VÍCE JAK 1300 KLIENTŮ

99,8% SPOKOJENOST S PODPOROU

MINDFORGE

NSM NETWORK SECURITY MONITORING CLUSTER

Microsoft Partner

SODAT

www.sodat.com

CO DĚLÁME?

SODAT PROTECTION

MONITORING A RESTRIKCE

SODAT ANALYTICS

POKROČILÁ ANALYTIKA

SODAT ENCRYPTION

OCHRANA ŠIFROVÁNÍM

PROČ TUTO OBLAST ŘEŠÍME?

SODAT

PROTOŽE JE TO DŮLEŽITÉ?

Nejrychleji rostoucí hrozby jsou rizika spojená s uživateli

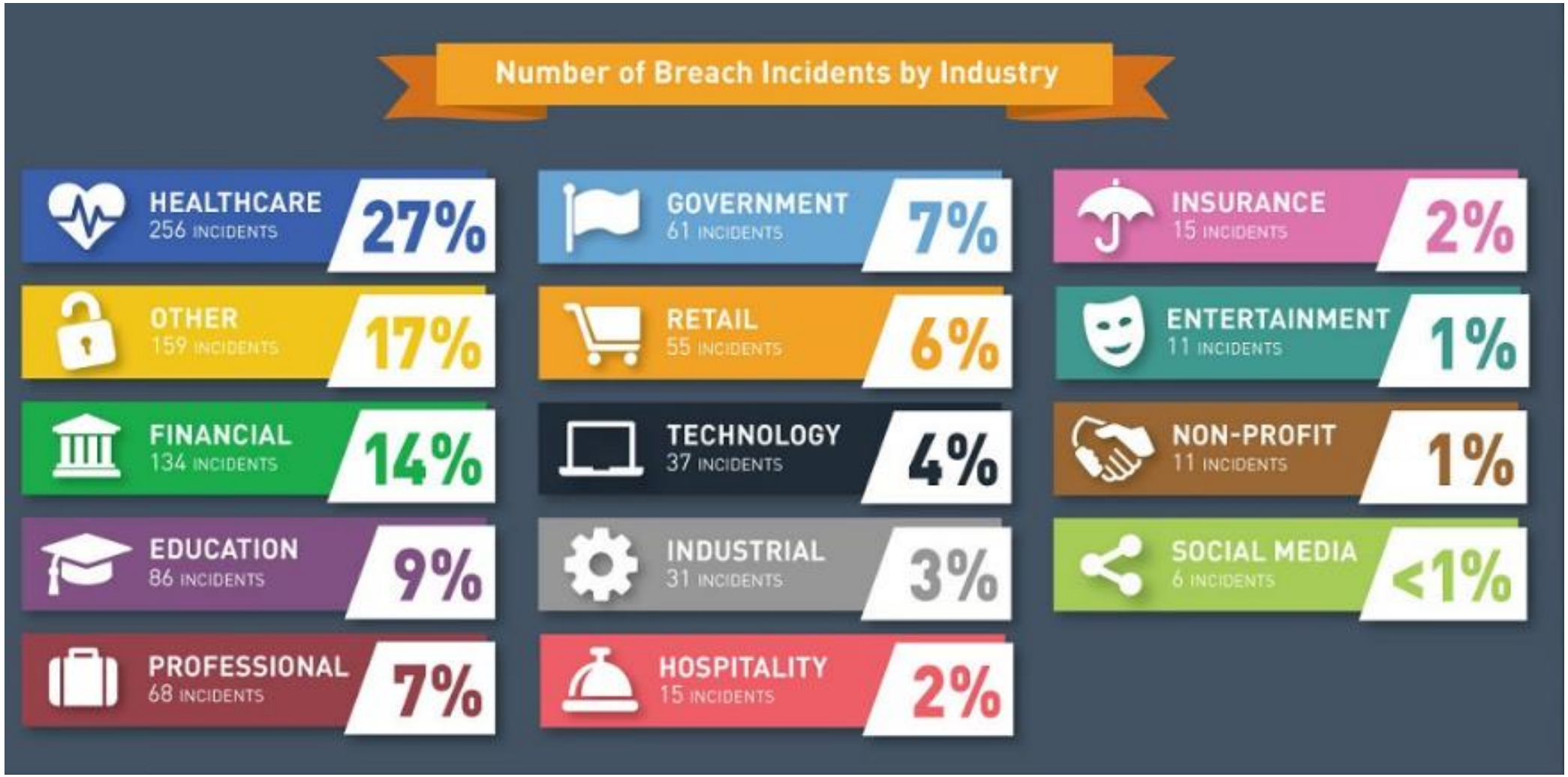
Nejhůře se zabraňuje útokům

Pozornost organizací se upírá od prevence ke schopnosti řešit incidenty

Perimetr zvenčí je dobře chráněn a nyní je prostor se věnovat novým bezpečnostním výzvám

Uživatelská rizika jsou nejvíce podceňovaná a bagatelizovaná

KDE SE NEJVÍC „KRADE“?



SODAT

Zdroj: Gemalto

KONKRÉTNÍ PŘÍPAD
...aneb JAK TO BYLO?

SODAT

ULOZ.TO

KAM?

SODAT

NA ULOZ.TO

aneb KDO BY TO TAM HLEDAL?

BYLO NEBYLO

ADMIN: Dochází ti místo ve schránce. Udělej si zálohu.

USER: Jak?

ADMIN: Normálně v Outlooku dej archivovat.

USER: Kam to mám uložit?

ADMIN: Mně je to jedno hlavně ať to pak najdeš. Třeba na nějaký server.

USER: **(myšlenka)** hmmm „Server?“ No znám uloz.to, to je přece fajn server a taky bezpečný mají https ☺ A kdo by to tam hledal?

BYLO

Počet záloh poštovních schránek:	111, pouze jedna chráněná heslem
Firemních:	80 %
Počet kompromitovaných dokumentů:	více jak 10 000
Objem dat:	více jak 3.5 GB dat v přílohách
Počet příjemců:	2 440
Kompromitovaných domén:	1 162
Obsah dokumentů:	Hesla, mzdy, smlouvy, faktury zdravotní dokumentace, ŘC
Zdravotní péče:	4 organizace (obrat 6 mld.)

OSOBNÍ ÚDÁJE VEŘEJNĚ A BEZ OBAV?

Odpovědět Odpovědět všem Přeposlat

[redacted]

Tato zpráva se přeposlala nebo se na ni poslala odpověď.

_20180830_071004.JPG 109 KB | _20180830_071056.JPG 104 KB | _20180830_071158.JPG 109 KB

Dobry[redacted]
(omlouvam se ze nepouzivam hacky a carky, ale nemam je tady:-D)
Moc dekuji za informace co ste mi poslala, je to super cteni a opravdu hodne informaci takze za to sem opravdu rada
ta moznost, myslite ze by bylo mozne v pondeli[redacted] Ale muzu se prispusobit takze kolem toho datumu by to slo i

Prikladam fotky, doufam ze budou stacit. Cetla sem si o tehle procedure uz asi rok a konecne sem se k tomu odhodla
je urcite skvela moznost jak tomu pomoct a kdyby to slo o cislo nahoru tak bych skakala radosti ale chapu ze se neja

- [redacted]
- Jsem zdrava nemam zadne zdravotni potize a ani nekourim

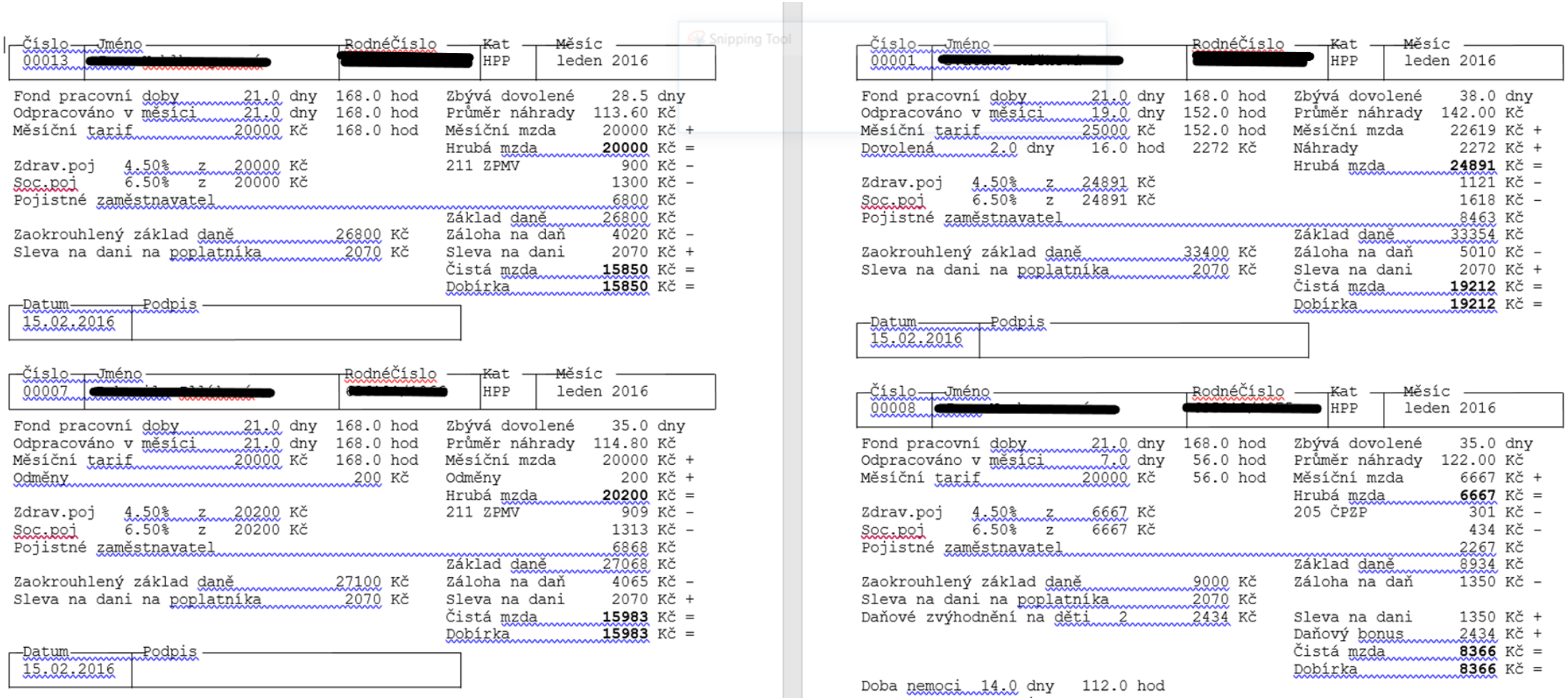
(jako mala sem mela selest na srdci ale bylo mi receno ze to bylo tak male ze to nicemu nevadi a nemela sem nikdy

Moc Dekuji a budu se tesit na dalsi email.
Preji Krasny den
[redacted]

SODAT

www.sodat.com

OSOBNÍ ÚDÁJE VEŘEJNĚ A BEZ OBAV?



Číslo	Jméno	RodnéČíslo	Kat	Měsíc
00013	[redacted]	[redacted]	HPP	leden 2016

Fond pracovní doby	21.0 dny	168.0 hod	Zbývá dovolené	28.5 dny	
Odpracováno v měsíci	21.0 dny	168.0 hod	Průměr náhrady	113.60 Kč	
Měsíční tarif	20000 Kč	168.0 hod	Měsíční mzda	20000 Kč	+
			Hrubá mzda	**20000** Kč	=
Zdrav.poj 4.50% z	20000 Kč		211 ZPMV	900 Kč	-
Soc.poj 6.50% z	20000 Kč			1300 Kč	-
Pojistné zaměstnavatel				6800 Kč	
			Základ daně	26800 Kč	
Zaokrouhlený základ daně	26800 Kč		Záloha na daň	4020 Kč	-
Sleva na dani na poplatníka	2070 Kč		Sleva na dani	2070 Kč	+
			Čistá mzda	**15850** Kč	=
			Dobírka	**15850** Kč	=

Datum	Podpis
15.02.2016	

Číslo	Jméno	RodnéČíslo	Kat	Měsíc
00007	[redacted]	[redacted]	HPP	leden 2016

Fond pracovní doby	21.0 dny	168.0 hod	Zbývá dovolené	35.0 dny	
Odpracováno v měsíci	21.0 dny	168.0 hod	Průměr náhrady	114.80 Kč	
Měsíční tarif	20000 Kč	168.0 hod	Měsíční mzda	20000 Kč	+
Odměny	200 Kč		Odměny	200 Kč	+
			Hrubá mzda	**20200** Kč	=
Zdrav.poj 4.50% z	20200 Kč		211 ZPMV	909 Kč	-
Soc.poj 6.50% z	20200 Kč			1313 Kč	-
Pojistné zaměstnavatel				6868 Kč	
			Základ daně	27068 Kč	
Zaokrouhlený základ daně	27100 Kč		Záloha na daň	4065 Kč	-
Sleva na dani na poplatníka	2070 Kč		Sleva na dani	2070 Kč	+
			Čistá mzda	**15983** Kč	=
			Dobírka	**15983** Kč	=

Datum	Podpis
15.02.2016	

Číslo	Jméno	RodnéČíslo	Kat	Měsíc
00001	[redacted]	[redacted]	HPP	leden 2016

Fond pracovní doby	21.0 dny	168.0 hod	Zbývá dovolené	38.0 dny	
Odpracováno v měsíci	19.0 dny	152.0 hod	Průměr náhrady	142.00 Kč	
Měsíční tarif	25000 Kč	152.0 hod	Měsíční mzda	22619 Kč	+
Dovolená 2.0 dny	16.0 hod	2272 Kč	Náhrady	2272 Kč	+
			Hrubá mzda	**24891** Kč	=
Zdrav.poj 4.50% z	24891 Kč			1121 Kč	-
Soc.poj 6.50% z	24891 Kč			1618 Kč	-
Pojistné zaměstnavatel				8463 Kč	
			Základ daně	33354 Kč	
Zaokrouhlený základ daně	33400 Kč		Záloha na daň	5010 Kč	-
Sleva na dani na poplatníka	2070 Kč		Sleva na dani	2070 Kč	+
			Čistá mzda	**19212** Kč	=
			Dobírka	**19212** Kč	=

Datum	Podpis
15.02.2016	

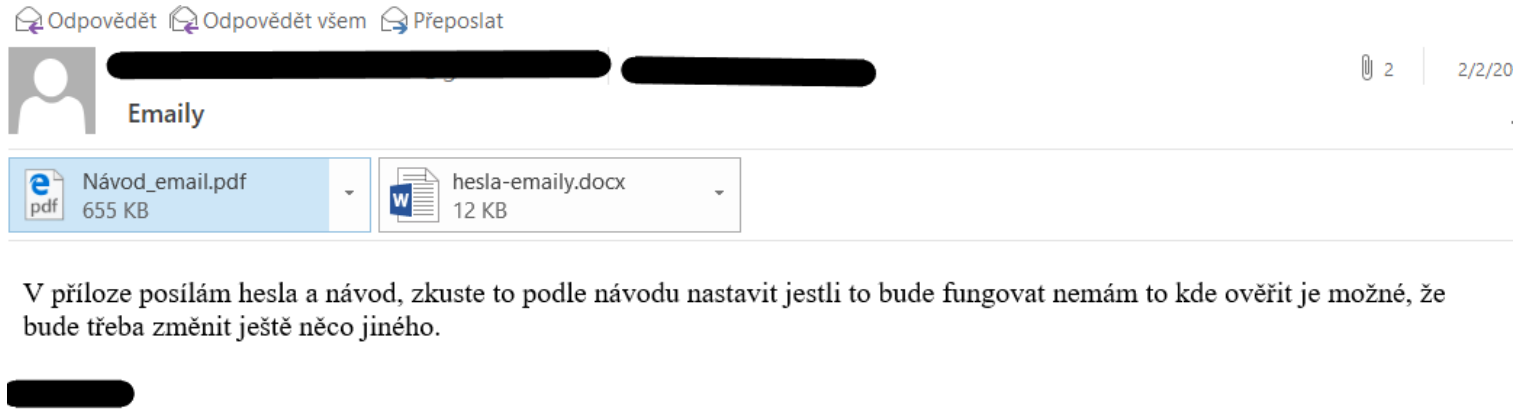
Číslo	Jméno	RodnéČíslo	Kat	Měsíc
00008	[redacted]	[redacted]	HPP	leden 2016

Fond pracovní doby	21.0 dny	168.0 hod	Zbývá dovolené	35.0 dny	
Odpracováno v měsíci	7.0 dny	56.0 hod	Průměr náhrady	122.00 Kč	
Měsíční tarif	20000 Kč	56.0 hod	Měsíční mzda	6667 Kč	+
			Hrubá mzda	**6667** Kč	=
Zdrav.poj 4.50% z	6667 Kč		205 ČPZP	301 Kč	-
Soc.poj 6.50% z	6667 Kč			434 Kč	-
Pojistné zaměstnavatel				2267 Kč	
			Základ daně	8934 Kč	
Zaokrouhlený základ daně	9000 Kč		Záloha na daň	1350 Kč	-
Sleva na dani na poplatníka	2070 Kč				
Daňové zvýhodnění na děti 2	2434 Kč		Sleva na dani	1350 Kč	+
			Daňový bonus	2434 Kč	+
			Čistá mzda	**8366** Kč	=
			Dobírka	**8366** Kč	=
Doba nemoci 14.0 dny	112.0 hod				

SODAT

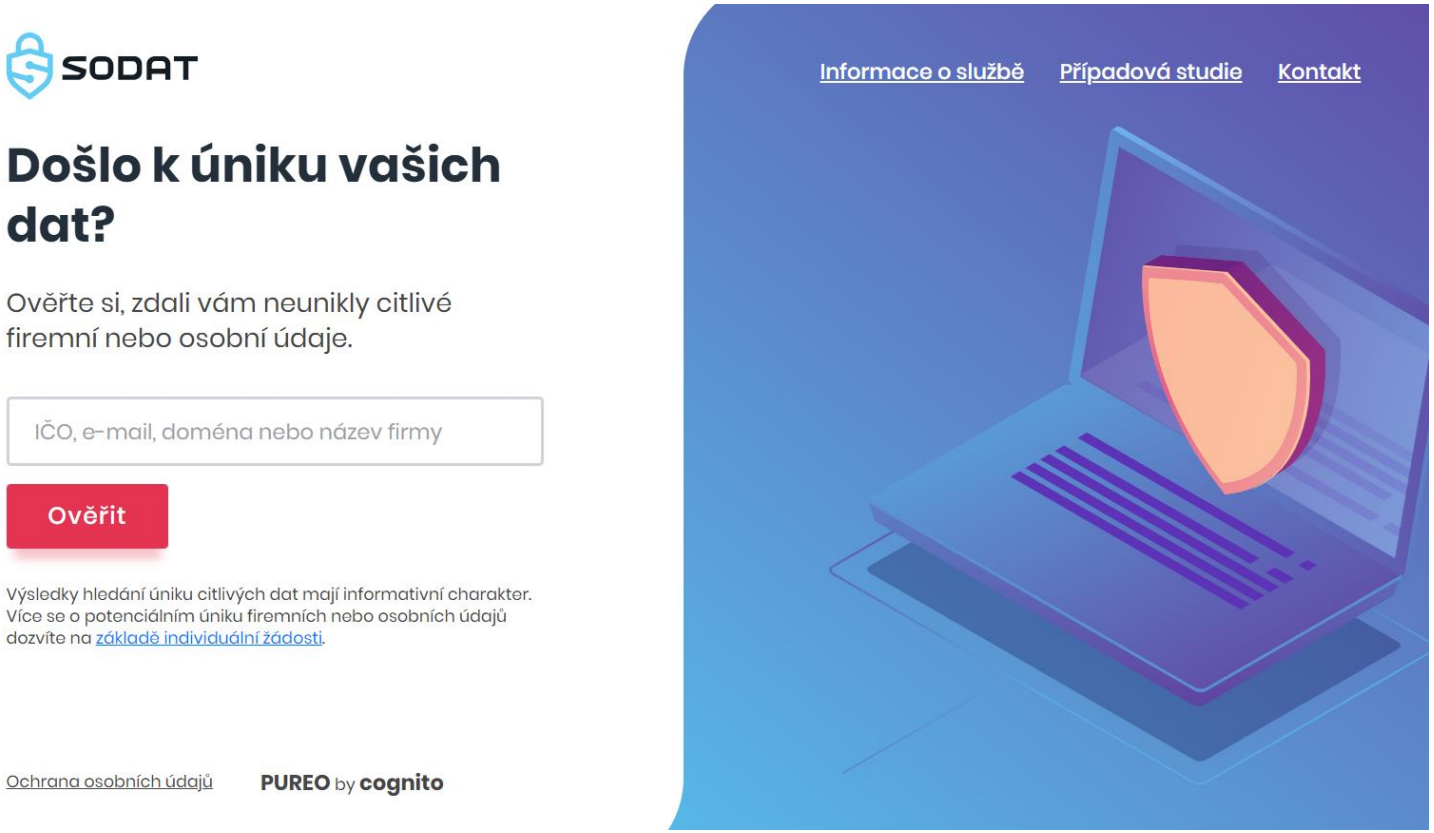
www.sodat.com

PERLA NA KONEC



TÝKÁ SE TO I VÁS?

https://unik-dat.sodat.com/



CO S TÍM, KAM DÁL?

- Změňte zaměření bezpečnosti z **control-centric na human-centric**.
- Zaměřte se na **informační bezpečnost**, nejen na síťovou bezpečnost (zabezpečení sítě).
- Zvyšujte schopnosti **detekcí/monitorování a adekvátních reakcí.**
- Zkontrolujte, zda zaměstnanecké pracovní smlouvy obsahují **oblast zabezpečení dat.**
- Ujistěte se, že vaši dodavatelé mají **silné zabezpečení.**

JAKÉ SITUACE ŘEŠÍ SODAT?

Prevence ztráty informací

Vizibilita nad pohybem dat

Upozornění na nebezpečné aktivity

Ochrana dat v místě uložení

Naplnění legislativních nařízení

JAK JE ŘEŠÍ?

Monitoring pohybu dat v organizaci

Vyhodnocení bezpečnostních incidentů

Citlivá data opouštějící organizaci

Řízení externích zařízení a práv uživatele

Napojení na centrální dohledová centra (SIEM, LOG management)

Ochrana dat šifrováním na koncových stanicích / serverech / ext. Dev.

Detekce anomálií v zacházení s daty

PŘÍPADOVÁ STUDIE

Nemocnice Tábor

SODAT

VÝCHOZÍ STAV

- **Potřeba efektivního nástroje na pokročilou analýzu koncových stanic**
  - Nemožnost kontroly činnosti uživatele a využívání koncových stanic
  - Nedostatek informací pro plánování dalšího rozvoje IS/IT

- **Potřeba nastavení bezpečnostních pravidel při zacházení s daty**
  - Omezení bezpečnostních hrozeb, zejména chyb na straně uživatele
  - Omezení bezpečnostních hrozeb, které představují nevyžádaný software

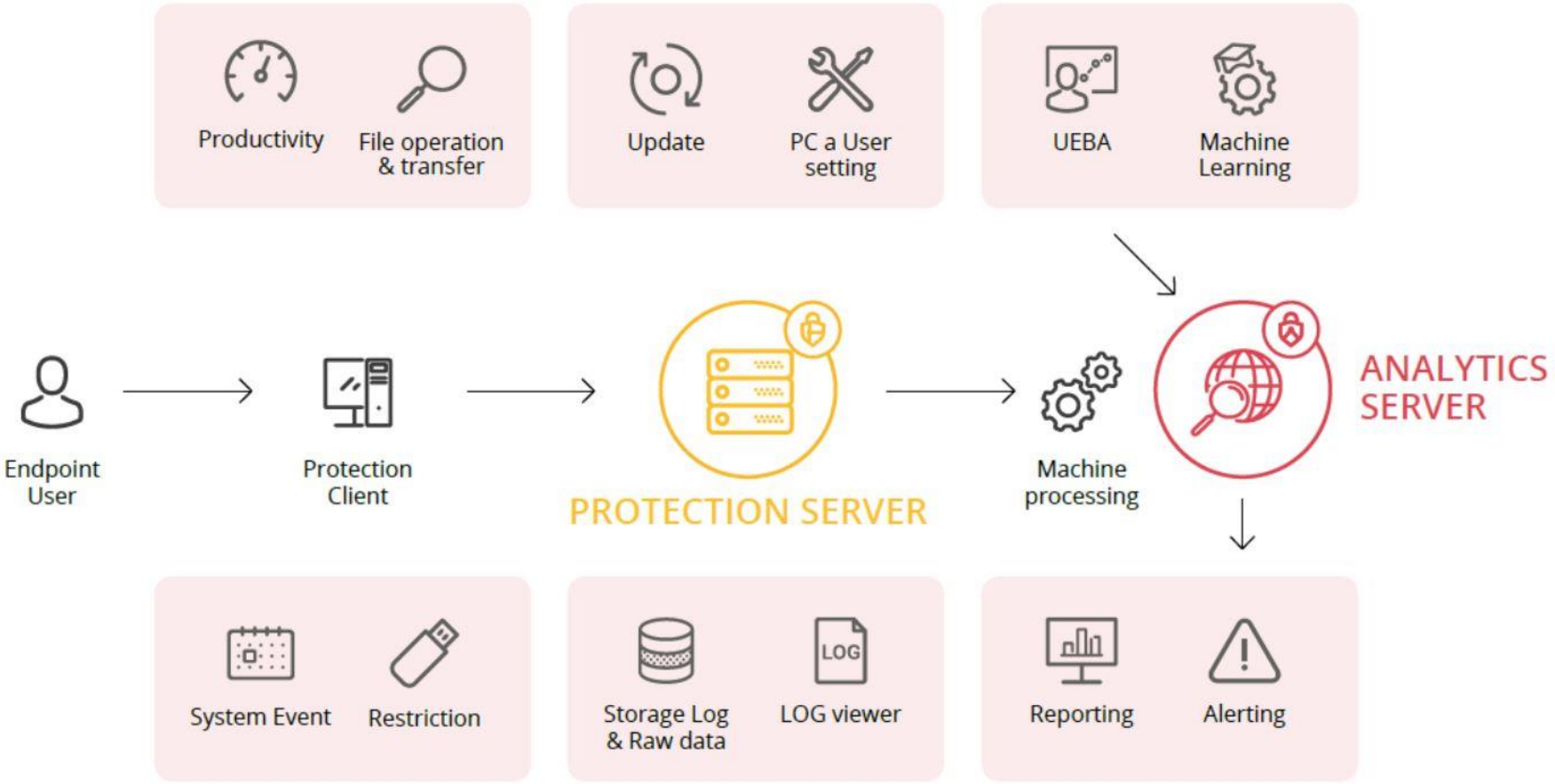
- **Soulad se strategií dalšího rozvoje v oblasti kybernetické bezpečnosti**

  - Dobrá zkušenost z přechozích generací produktu
  - Možnost napojení do centrálního nástroje pro vyhodnocení dat (SIEM)

PRŮBĚH IMPLEMENTACE

- Implementace probíhala za asistence konzultanta ze společnosti SODAT, stačil rozsah jednoho dne
- Veškeré úkony byly prováděny vzdáleně bez nutnosti přímé alokace našich pracovníků
- Instalace na koncové stanice probíhala průběžně bez narušení rutinní činnosti uživatele
- Rozsah nasazení je cca 450 stanic

ŘEŠENÍ SODAT



KOMU JSME POMOHLI

Veřejná správa	Finanční segment	Komerční segment	Segment zdravotnictví

úřad pro ochranu osobních údajů
the office for personal data protection

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo obrany České republiky

Ministerstvo financí České republiky

Úřad vlády České republiky

MĚSTO TEPLICE

OSTRAVA!!!

PENZIJNÍ SPOLEČNOST ČESKÉ SPOŘITELNY

Česká průmyslová zdravotní pojišťovna

SLAVIA POJIŠŤOVNA

KB Pojišťovna

BERNARD

TORAY Innovation by Chemistry

ZEZ SILKO

OLYMPUS

ČESKÝ AEROHOLDING

VKS LEGAL ADVOKÁTNÍ KANCELÁŘ

DAIDO METAL

BONATRANS

wanzl

TM T Machinery a.s.

IVECO

dpmo

KOH-I-NOOR

BEZNOSKA We bring back joy to movement

ABAS IPS MANAGEMENT

Nemocnice Vyškov

NT+ Nemocnice Tábor, a. s.

AGEL

ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA KRAJE VYSOČINA

SODAT

www.sodat.com

DĚKUJI ZA POZORNOST

www.sodat.com