IT jako nástroj pomsty neloajálního zaměstnance

JUDr. Karel Antonín Kodeda
Mgr. Barbora Gaveau, LL.M.
Mgr. Martin Leskovjan

21. června 2018

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

Úvod - praktické dopady elektronizace na bezpečnost organizací

JUDr. Karel Antonín Kodeda
Mgr. Barbora Gaveau, LL.M.
Mgr. Martin Leskovjan

Úvod – pojem práva a morálky I

- Právo je normativní způsobem regulace společenských vztahů garantovaných státní mocí.
- Představuje systém společenských příkazů, zákazů a dovolení stanovících, co má být.
- Neposkytuje však regulaci všech vztahů ve společnosti. Právem chce společnost regulovat nejdůležitější vztahy.

Pojem práva a morálky II

- Může právo předběhnout a nahradit morálku v právech osoby? (homosexualita, eutanazie, interrupce, náhradní mateřství)
- Může právo předběhnout a nahradit morálku ve veřejnoprávní oblasti, jako jsou diplomacie, zpravodajské služby, jejich technické, finanční a personální zajištění, terorismus, organizovaný zločin, extremismus, ochrana ekonomických a hospodářských zájmů, postup proti zpravodajským službám cizí moci?

Pojem práva a morálky III

Kombinace vztahů morálky a práva se projevují v různých právních systémech:

- “přednost“ práva před morálkou – normativní právo
- “přednost” morálky nad právem – common law
- prolínání se morálky a práva – například jako jednání mimoprávní

Pojem práva a morálky IV

Byť by se právní teorie snažila závislosti na mravech a morálce vyhnout a založit platnost práva jen na procesní správnosti a ústavnosti, ukazuje se, že právo se bez morálky neobejde.

Digitalizace I – Průmysl 4.0

- čtvrtá průmyslová revoluce
- vyšší zranitelnost ze strany kyberútoků, které mohou cílit nejen na know-how a další citlivé informace, ale mohou způsobovat i výpadky ve výrobě nebo narušení podnikání firem
- vyšší nároky na zajištění IT bezpečnosti, spolehlivosti důležitých systémů, integritu procesů
- změna vnitřních procesů a postupů

Digitalizace II

- Digitalizace zpravidla vede k outsoursingu, části IT služeb.
- Paradox: společnosti mívají větší pocit bezpečí, je-li jejich IT tzv. „in house“
- Dva základní praktické dopady:
  - jak elektronická data ochránit před zneužitím
  - jak s elektronickými daty nakládat , abychom je zachovali po potřebnou dobu

=> bezpečnost a spolehlivost

Tři cíle týkající se bezpečnosti a spolehlivosti

- Důvěrnost elektronických dat
- Integrita elektronických dat
- Dostupnost elektronických dat

=> tyto cíle spolu úzce souvisejí a pomůžou pochopit regulaci týkající se digitalizace a kybernetické bezpečnosti

Kybernetická bezpečnost v praktických souvislostech Současné trendy IT zabezpečení v organizacích

Martin Leskovjan

CITADELO

FLYEYE

Paralelní Polis

OSNOVA

- Jsou zaměstnanci skutečně hrozba?
- Bez-vědomí a jak ho odstranit
- Management rolí v organizaci
- Záznamy o aktivitách a dokumentace
- Monitoring a detekce
- Pasti, pasti, pastičky
- Systémoví administrátoři a další privilegovaní uživatelé
- Zálohování a obnova
- Deprovisiong

JSOU ZAMĚSTNANCI SKUTEČNĚ HROZBOU?

2004 ECrime Watch Survey: 29%

2011 CyberSecurity Watch Survey: 46%

2015 IBM Report: 44,5%

2016 U.S. State of Cybercrime report: 43%

2017 U.S. State of Cybercrime report: 20%

RIZIKA 4.0

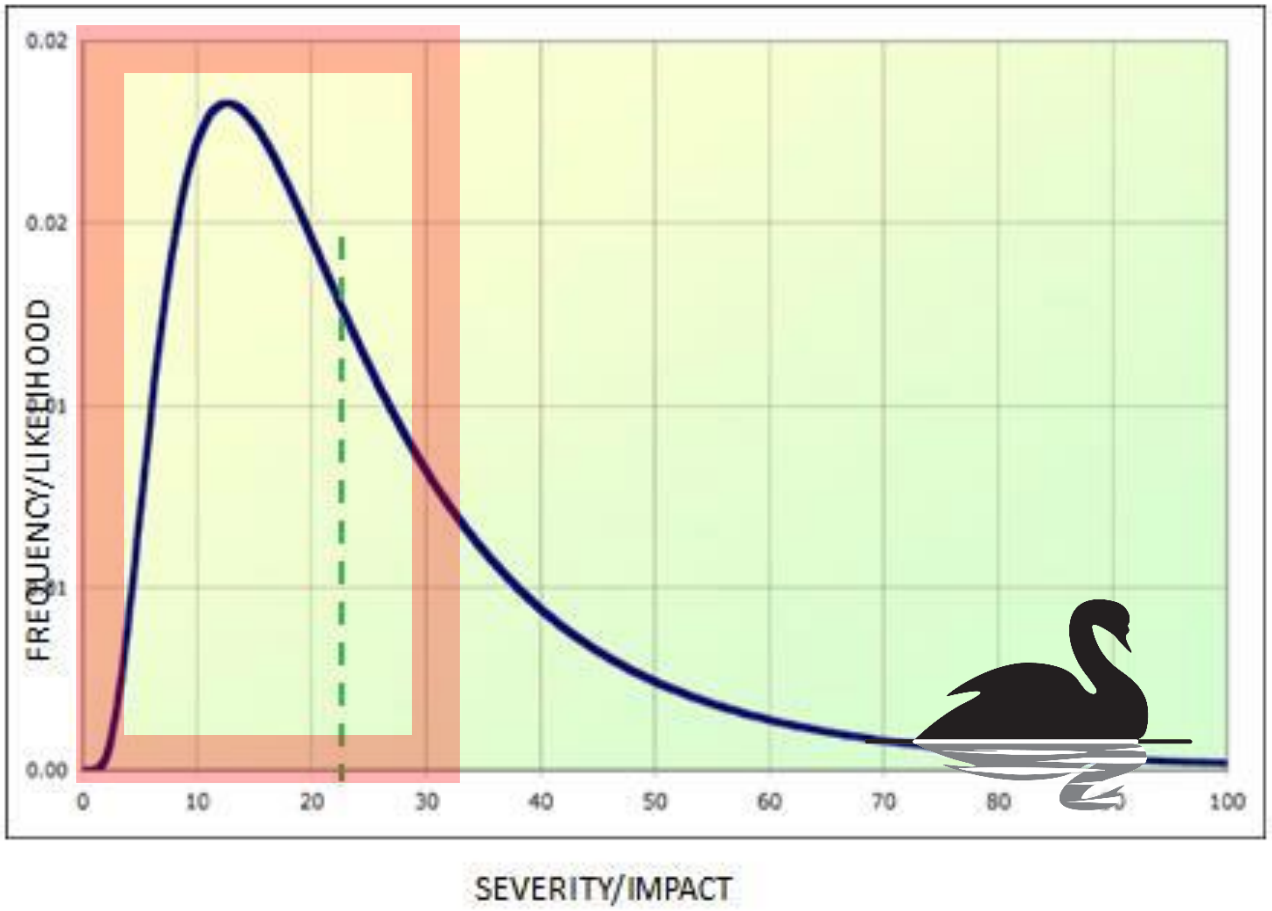
RIZIKO = PRAVDĚPODOBNOST * DOPAD

RIZIKO = [redacted] DOPAD

Fragilita vs. antifragilita

NASSIM NICHOLAS TALEB
- Černá labuť
- Antifragilita
- Skin in the game

RIZIKA 4.0


0.02
0.02
0.00
FREQUENCY/LIKELIHOOD
0
10
20
30
40
50
60
70
80
100
SEVERITY/IMPACT

RIZIKA 4.0

- vzdálené řízení (remote control)
- digitalizace všech složek
- komplexita
- řízení fyzických procesů
- asymetrie sil obrana / útok

BEZ-VĚDOMÍ A JAK HO ODSTRANIT

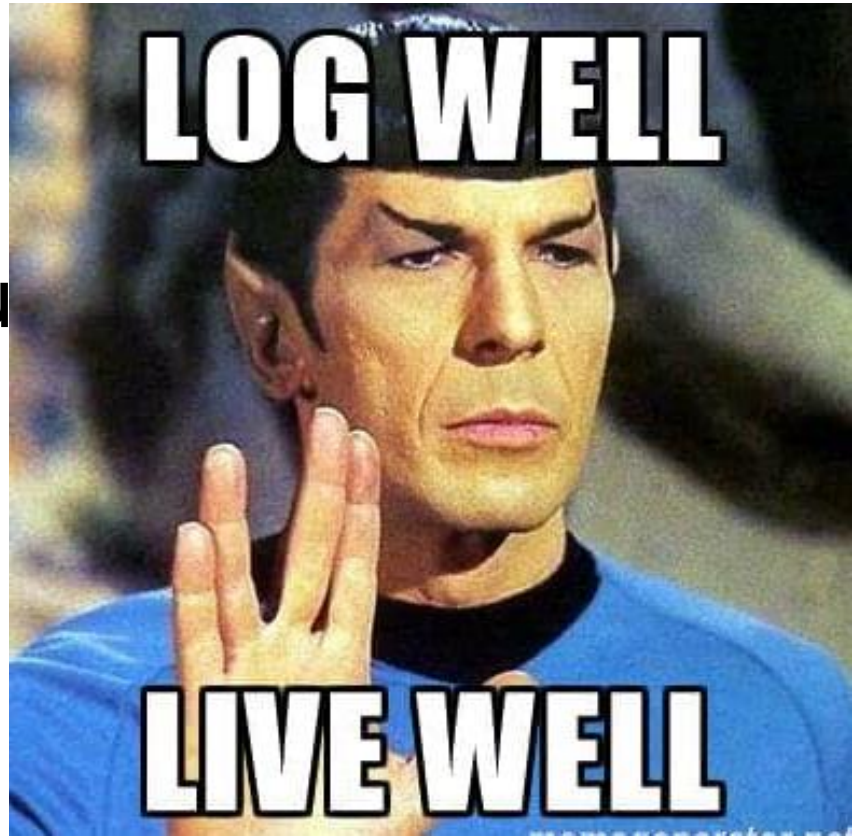
- nejúčinnější ochranou před insiderem jsou jeho kolegové
- pravidelný tréning všech zaměstnanců
- seznámení s:
  - interními pravidly
  - principy sociálního inženýrství
  - přísnou politikou hesel a přístupů

MANAGEMENT ROLÍ

- separace odpovědností
- minimalizace privilegií
- pravidlo čtyř očí
- management konfigurací (distribuce SW a change management)
- kontrola fyzického přístupu

ZÁZNAMY O AKTIVITÁCH A DOKUMENTACE

- LOG? -> ON!
- IT i fyzické
- audity klíčových prvků infrastruktury
- uchování záznamů



MONITORING A DETEKCE

- IPS / IDS
- SIEM
- automatický / manuální
- SOC

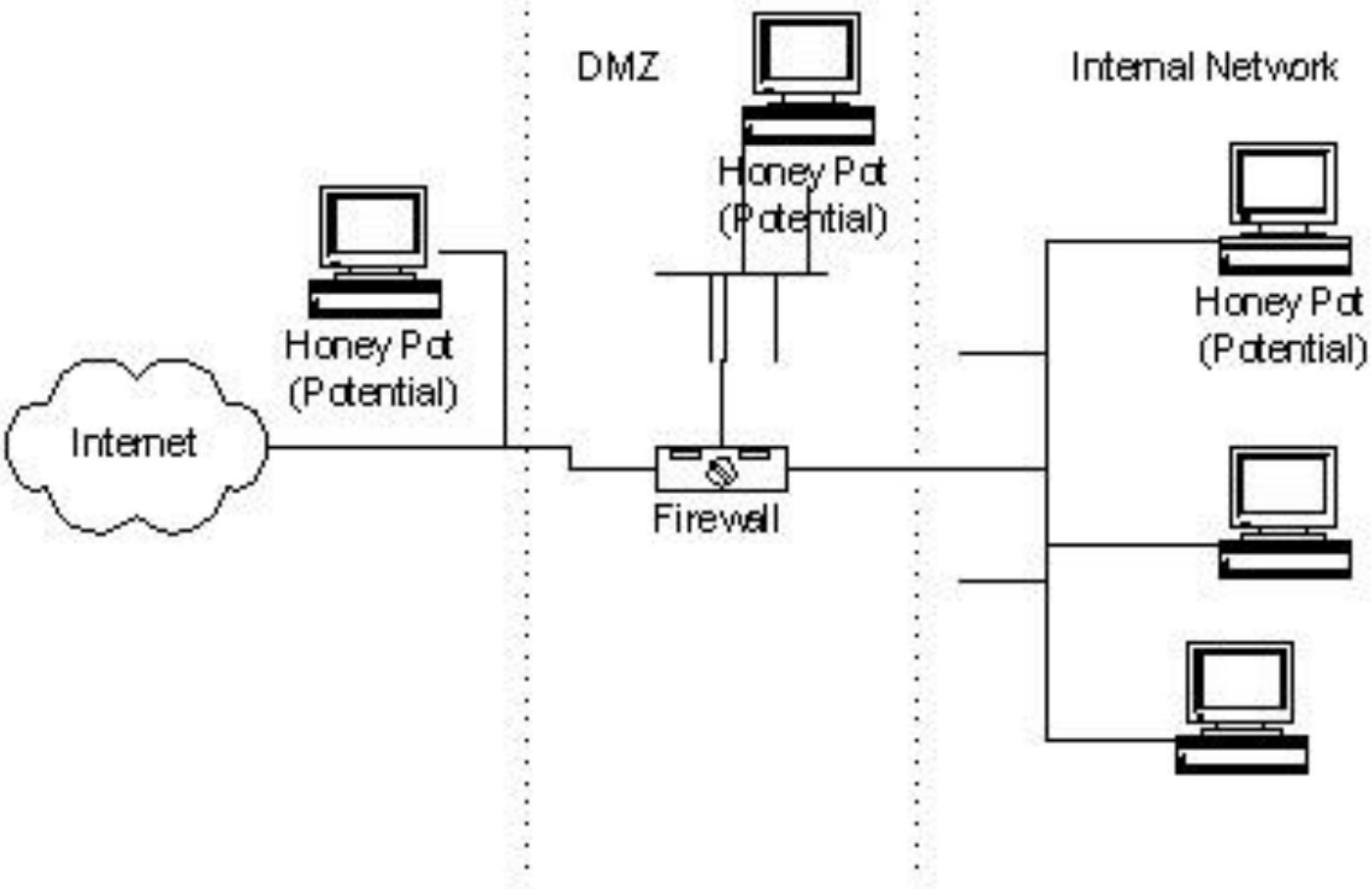
MONITORING A DETEKCE

Demo: Terramind

PASTI, PASTI, PASTIČKY

HONEYPOT

PASTI, PASTI, PASTIČKY



SYSTÉMOVÍ ADMINISTRÁTOŘI A DALŠÍ PRIVILEGOVANÍ UŽIVATELÉ

- ochrana záznamů před manipulací
- zvýšená odpovědnost a background check
- honeypot
- zvýšená bezpečnost autenfikace
- pravidlo čtyř očí
- multisignature

ZÁLOHOVÁNÍ A OBNOVA

- tréning obnovy po kompletním výpadku
- ochrana před smazáním
- prevence krádeže fyzických médií
- integrity check

DEPROVISIONING

- management rolí
- detailní proces s odpovědnostmi
- pravidelný tréning
- implementace Active Directory / LDAP

SHRNUTÍ

- pravidelné školení
- jasné role a kompetence
- záznamy
- pozor na klíčové pracovníky
- monitorujte!
- zálohujte a obnovujte

Děkuji za pozornost!

© 2018

Tento seminář pořádá
Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz

Řízení vnitřních procesů a vnitřní předpisy pro využívání ICT

JUDr. Karel Antonín Kodeda
Mgr. Barbora Gaveau, LL.M.

Úvod

- charakteristika vnitřního předpisu a jeho úloha
- které vnitřní předpisy jsou s ohledem na elektronizaci nejdůležitější
- praktická doporučení k ochraně dat společností

Vnitřní předpisy charakteristika I

- obecná úprava – zákoník práce §305
- vnitřní předpis stanovit mzdová nebo platová práva a ostatní práva v pracovněprávních vztazích
- vnitřní předpis je závazný pro zaměstnavatele a pro všechny jeho zaměstnance
- vnitřní předpis musí být všem zaměstnancům zaměstnavatele přístupný
- zaměstnavatel je povinen uschovat vnitřní předpis po dobu 10 let ode dne ukončení doby jeho platnosti
- některé předpisy nebo jejich přílohy mohou obsahovat utajované informace a pak mají zvláštní režim zveřejnění a ochrany

Vnitřní předpisy charakteristika II

- tvorba vychází z obecných zásad pro tvorbu právních předpisů, mívají různá označení (interní předpis, řád, směrnice, pokyn, vnitřní normativní akt, řídicí dokument apod.)
- operativní předpisy – slouží k operativnímu vydání řídícího ustanovení zpravidla řeší konkrétní situaci nebo problém
- normativní předpisy (řád, směrnice , pracovní postup) předpisy s relativně dlouhodobou platností, postihující jak statickou, tak dynamickou stránku organizace, řešící zejména uspořádání organizační struktury, kompetence, průběh procesů a pokyny k zajištění jejich správného průběhu
- technické předpisy (výrobní dokumentace, technická norma týkající se technické a technicko-provozní stránky strojů a zařízení, provozních objektů a technických řídicích systémů, technické předpisy s utajovanými informacemi)

Zaměstnanci a vnitřní předpisy

- zaměstnanci jsou povinni dodržovat předpisy vztahující se k práci jimi vykonávané, pokud s nimi byli seznámeni § 301 písmeno c) zákoníku práce a § 302
- adresné vymezení povinností zaměstnance ve vnitřních předpisech, základními vnitřními předpisy jsou:

- organizační řád

- pracovní řád

- podpisový řád

- spisový a skartační řád

- srozumitelné nastavení pravidel a prevence ex ante je účinnější než sankce, soudy a postihy ex post

Vnitřní předpisy - Řád pro vydávání předpisů

- definování soustavy a druhů vnitřní předpisů
  - operativní
  - normativní
  - technické
- zásady tvorby vnitřních předpisů
- spolupráce a součinnost při vydávání vnitřních předpisů (vazba na organizační řád)
- grafické zpracování a forma
- evidence, publikace v listinné a v elektronické podobě

Vnitřní předpisy - Pracovní řád

- upravuje pouze blíže povinnosti vyplývající z právních předpisů, které se vztahují na vykonávanou práci, více do detailu je rozvádí
- bezpečnost a ochrana zdraví při práci
- ochrana majetku , ochrana nehmotného vlastnictví zaměstnavatele
- důvěrnost informací
- ochrana osobních údajů

Vnitřní předpisy - Organizační řád

- způsob řízení, působnost a struktura orgánů společnosti, poradní orgány a komise
- obchodní řízení společnosti
- zásady řízení – strategické, projektové
- formy řízení – přímé řízení a organizační stupně
  – procesní řízení a jeho formy
- základní dokumenty a vnitřní předpisy společnosti
- organizační struktura a působnost vnitřních útvarů řízení změn
- přílohy: organizační schémata, mapa procesů a vymezení odpovědností

Vnitřní předpisy - Spisový a skartační řád

- souhrn předpisů pro vedení spisové služby a související pojmy:
  - dokument
  - původce
  - spisové znaky
  - skartační znak
  - skartační lhůta
- spisový plán / skartační plán
- uchovávání některých dokumentů po skončení skartační lhůty
- 7 etap života dokumentu

Vnitřní předpisy - Podpisový řád I

- podpisová oprávnění ve vnitřním styku
- administrativní úkony uvnitř společnosti
- zásady podepisování – např. zásada čtyř očí
- účetní úkony
- podpisová oprávnění ve vnějším styku
    - smlouvy týkající se nabývání a zcizování majetku
    - obchodní smlouvy
    - úkony k orgánům státní správy a soudům
    - korespondence společnosti

Vnitřní předpisy - Podpisový řád II

- postup při opatřování elektronického podpisu pro zaměstnance
- elektronický podpis ve vnitřním styku
- elektronický podpis ve vnějším styku
- používání elektronických prostředků při schvalování písemností
- používání elektronického podpisu při podepisování
- přílohy – postup při vydávání plné moci
- jiná pověření

Praktická doporučení – která data chránit

- chráněné informace, nehmotné vlastnictví společnosti ve vnitřních předpisech společnosti:
  - know-how, vlastní výzkum, vývoj, výrobní a pracovní postupy, vztahující se k produktům a službám společnosti
  - marketingové informace – strategie firmy, cílové skupiny klientů/odběratelů, analýzy apod.
  - obchodní informace – seznamy klientů/odběratelů, objemy a trendy obchodu apod.
  - detailní finanční výsledky
  - různé strategické analýzy a klíčová rozhodnutí vedení firmy
  - osobní údaje

Praktická doporučení na zvýšení bezpečnosti dat vně společnosti

- kdo a za jakých podmínek má přístup k poskytnutým informacím a datům, osobním údajům a kde budou uložena (pozor na přeshraniční předávání – server v zahraničí)
- je poskytovatel služby auditován a držitelem mezinárodně uznávaných bezpečnostních certifikátů
- kontrola místa/míst s uloženými daty/aplikacemi
- technická a právní odpovědnost za bezpečnost, opatření při porušení bezpečnosti
- používané šifrování dat či jiná opatření z hlediska právních požadavků a bezpečnosti (anonymizace, pseudoanonymizace, fragmentace apod.)
- opatření proti ztrátám v případě kolapsu
- opatření pro případ ukončení činnosti poskytovatele služeb, další osud poskytovaných dat /aplikací
- preventivní monitorování poskytovatelem služby jako ochrana proti podezřelým nebo protizákonným praktikám
- Servis Level Agreement (cenová ujednání, kvalitativní a kvantitativní záruky)

Praktická doporučení na zvýšení bezpečnosti dat uvnitř společnosti

- správně a důkladně formulované zaměstnanecké smlouvy a vnitřní předpisy v částech týkajících se užívání IT zaměstnavatele a zaměstnance
- správné vymezení vnitřních procesů a rozsah oprávnění zaměstnanců k dokumentům v elektronické podobě – zaměstnanec má mít přístup pouze k těm informacím, které potřebuje
- používání účinného software na vyhledávání anomálií v sítích, útoků virů, spam a nedovolených aplikací
- monitoring IT technologií a soustavné vyhodnocování jeho výsledků
- školení zaměstnanců o postupu při oznamování podezření ztráty dat nebo elektronických útoků
- ochrana proti přístupu k informačním technologiím společnosti cizími osobami
- obrana proti virům, malware, phishing
- bezpečnost a ochrana informačních technologií jako součást risk managementu
- organizování a vyhodnocování bezpečnostních auditů

Závěr

- To, co podmiňuje platnost papírových dokumentů, platí i pro dokumenty v elektronické podobě

- „Co platí off line, platí i on line“

Bezpečnost a spolehlivost při nakládání s dokumenty v elektronické podobě

Mgr. Barbora Gaveau, LL.M.

Úvod

- co má bezpečnost a spolehlivost IT zajišťovat
- co vlastně zabezpečuje elektronický podpis a časové razítko
- jaké jsou důsledky nedodržení zákonné úpravy

Utajení, diskrétnost a mlčenlivost

- obchodní tajemství (občanský zákoník)
- důvěrné informace (definované vnitřními předpisy a/nebo smlouvou)
- nehmotné vlastnictví (autorský zákon a práva z průmyslového vlastnictví)
- know-how technických a jiných postupů (definované vnitřními předpisy a/nebo smlouvou)
- osobní údaje (GDPR)

Bezpečnost IT se zabývá zabezpečením informací v počítačích a sítích

- zabezpečení ochrany před neoprávněným manipulováním se zařízeními počítačového systému
- ochrana dat před krádeží (i nelegální tvorba kopií dat) nebo poškozením
- bezpečná komunikace a přenos dat: kódování dat – kryptografie
- bezpečné uložení dat
- celistvost a nezměnitelnost dat

Spolehlivost IT

- minimum výpadků (nedostupnosti) jednotlivých prvků firemní IT infrastruktury, např. e-mailový systém, server, pracovní stanice
- vysoká dostupnost díky závislosti vnitřních procesů na informačních technologiích
- snižování ztrát v důsledku výpadků IT
- zálohování dat /infrastruktury pro řízení procesů v reálném čase

Nejčastější trestné činy v IT

- Podvod
- Vydírání
- Padělání

Základní požadavky na zachování důkazní síly elektronických originálů

- Základní požadavky na zachování důkazní síly elektronických dokumentů :
  - neporušitelnost obsahu (integrita, nesouvisí s formátem)
  - označení původce (autentičnost, věrohodnost původu)
  - čitelnost (přímo nebo prostřednictvím technického zařízení)

$\Rightarrow$ užití elektronického podpisu k právním úkonům včetně časového razítka a pečetě

Základní požadavky na zachování důkazní síly elektronických originálů

- Nový občanský zákoník 2014 § 562 odst. 2:

Má se za to, že záznamy o právních jednáních v elektronickém systému jsou spolehlivé, provádějí-li se systematicky a posloupně a jsou-li chráněny proti změnám.

- Nový občanský zákoník 2014 § 566 odst. 2:

Má se za to, že písemnosti týkající se právních skutečností, k nimž dochází při běžném provozu závodu, dokazují, dovolává-li se jich druhá strana k svému prospěchu, co je v listině obsaženo, a že listina byla vystavena v době na ni uvedené, to platí i v případě, že listina nebyla podepsána.

Základní požadavky na zachování důkazní síly elektronických originálů

Právní účinky elektronických podpisů (el.pečetí, el.čas. razítek), čl. 25 a násl. nařízení eIDAS č. 910/2014:

- Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.
- Kvalifikovaný **elektronický podpis** má právní účinek rovnocenný vlastnoručnímu podpisu. / U kvalifikované **elektronické pečeti** platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena. /U kvalifikovaného **elektronického časového razítka** platí domněnka správnosti data a času, které udává, a integrity dat, s nimiž jsou toto datum a tento čas spojeny.
- Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.

Právní účinky el. dokumentu

- elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu. (čl. 46 nařízení eIDAS)
- „elektronickým dokumentem“ je jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka (definice nařízení eIDAS)
- důkaz soukromou a veřejnou listinou

Jaký typ elektronického podpisu používat?

Zákon č. 297/2016 Sb. o službách vytvářejících důvěru §6:

(1) K podepisování elektronickým podpisem lze použít pouze uznávaný elektronický podpis, podepisuje-li se elektronický dokument, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti.

(2) Uznávaným elektronickým podpisem se rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis.

Jaký typ elektronického podpisu používat?

Zákon č. 297/2016 Sb. o službách vytvářejících důvěru §7:

K podepisování elektronickým podpisem lze použít zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu, podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 5 nebo § 6 odst. 1.

Podání podle zákona č. 500/2004 Sb., správní řád

Musí být podepsáno zaručeným elektronickým podpisem (§ 37 odst. 4), jinak je nutné podání do 5 dnů potvrdit, popřípadě doplnit písemně nebo ústně do protokolu anebo v elektronické podobě podepsané zaručeným elektronickým podpisem.

Ověřování platnosti

- Nařízení eIDAS a metodický návod MVČR pro ověřování platnosti EP a pečetí
- Existence časového razítka a pečeti
- Řetězení časových razítek
- Uchovávání dokladu o ověření

Důsledky nedodržení právní úpravy

- Neprokazatelnost právního jednání, snížení důkazní síly
  - Špatné zacházení s platným dokumentem po jeho vzniku - porušení důvěryhodné archivace
    - po technické stránce: nedoložení migrace formátu, žádné časové razítko nebo až po platnosti EP, jiný typ EP
    - nesprávná doba archivace
    - ztráta elektronického originálu z datové schránky po 90 dnech
- Neplatnost právního jednání
  - Nedodržení formy či jiné náležitosti právního jednání – např. dokument nebyl opatřen EP, podpisy na jedné listině nebo podepsala osoba neoprávněná

Směrnice na ochranu důvěrných informací a doporučená ustanovení pracovní smlouvy

JUDr. Karel Antonín Kodeda
Mgr. Barbora Gaveau, LL.M.

Úvod

- ✓ Nejčastější příčinou a zdrojem úniku informací jsou osoby fyzické
- ✓ Méně častým důvodem je selhání technické
- ✓ Na vytváření vnitřního předpisu se musí podílet všichni vedoucí zaměstnanci ve společnosti
- ✓ S předpisem musí být prokazatelně seznámeni všichni zaměstnanci
- ✓ Dbejte na definování a vymezení sankcí za porušení tohoto předpisu
- ✓ Všechny osoby přicházející do styku s informacemi společnosti vycvičit ve znalosti co nesmím / co musím – z anglického TO DO DO NOT

Důvod úniku chráněných informací způsobené zaměstnanci

- ✓ Úmysl
- ✓ Nedbalost
- ✓ Neznalost

Koho se směrnice týká

- Vlastníků společnosti
- Vedoucích zaměstnanců
- Zaměstnanců
- Externích spolupracovníků
- Obchodních partnerů
- Účastníků seminářů
- Návštěv ve společnosti

Některé zásady podnikové kultury I

- Důvěrné informace jsou součást nehmotného vlastnictví společnosti
  - Mohou zvýhodnit konkurenty
  - Jsou drahé
  - Musí být chráněny

- Kde se důvěrné informace nacházejí
  - V písemnostech společnosti
  - V informačních systémech společnosti
  - Na webových stránkách společnosti

Některé zásady podnikové kultury II

- Ochrana vlastních informací
  - Součást podnikové kultury
  - Součást bezpečnostní politiky společnosti
  - Součást procesu řízení rizik společnosti

- Respektování práv zaměstnavatele, soutěžitelů, dalších subjektů a jejich důvěrných informací
  - Důsledky porušení chráněných práv dalších subjektů fyzických osob zákon 40/2009 Sb.
  - Porušení vlastnických práv a trestní odpovědnost právnických osob zákon 418/2011 Sb.

Zásady ochrany důvěrných informací

Společnost má stanovit zásadu, že v případě nejistoty má být informace nejdříve považována za chráněnou!

- Ve společnosti je třeba mít anebo postupně vytvářet jedno místo/oddělení/zaměstnance, které/který odpovídá za klasifikaci důvěrných informací, za jejich uložení, archivaci a fyzickou ochranu
- Toto místo odpovídá na dotazy zaměstnanců v případě nejistoty o tom, zda je informace chráněná nebo nechráněná
- Rozhodovací působnost THE MUST DOCUMENTS AND MUST APPROVALS
- Vymezení kroků a postupů při odchodu zaměstnance ze společnosti (součinnost s útvarem HR)
- Definování a vymezení sankcí za porušení
- Všechny osoby přicházející do styku s informacemi společnosti vycvičit ve znalosti co nesmím /co musím – z anglického TO DO DO NOT

Děkuji za pozornost!

© 2018

Tento seminář pořádá

Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz