ZDRAVOTNICKÉ INFORMACE V OHROŽENÍ: ÚSPĚŠNÉ STRATEGIE PRO ZABEZPEČENÍ A OCHRANU OSOBNÍCH DAT VE ZDRAVOTNICTVÍ

David Houlding, Pavel Kubů, Intel

Rostoucí rizika, větší ohrožení, omezený rozpočet

Vyšší kvalita a nižší náklady na péči o pacienta závisejí na digitalizaci zdravotních záznamů a na přechodu na elektronické záznamy o pacientech. Tyto záznamy představují typ citlivých informací označovaných také jako elektronické chráněné zdravotní záznamy (electronic Protected Health Information–ePHR). Ve srovnání se svými papírovými ekvivalenty představují citlivé informace v elektronické podobě nová slabá místa. Bezpečnostní rizika a rizika spojená s ochranou citlivých informací se vlivem řady sílících trendů ve zdravotnictví zvyšují. K takovým rizikům patří např. mobilita lékařů a využívání bezdrátových sítí, výměna zdravotnických informací, cloudové aplikace, přístup typu „přineste si vlastní počítač" či používání osobních zdravotních záznamů (Personal Health Records–PHRs). Rafinovanost malwaru a bezpečnostní hrozby se neustále stupňují. K těmto problémům lze dále přiřadit omezené finanční prostředky, které mají zdravotnická zařízení k dispozici v oblasti snižování rizik, a zároveň zvyšující se závažnost důsledků případného selhání při ochraně citlivých informací.

Tato bílá kniha popisuje standardní postup, pomocí něhož mohou zdravotnická zařízení vyhodnotit rizika a zformulovat nutné požadavky na zabezpečení a ochranu dat. Nabízíme také několikavrstvou strategii hloubkové ochrany, která může zdravotnickým organizacím pomoci v průběhu životního cyklu hrozby snížit rizika a zabezpečit tak důvěrnost, celistvost a dostupnost citlivých informací. Na základě toho pak hovoříme o specifických bezpečnostních potřebách a potřebách ochrany dat ve zdravotnických organizacích a popisujeme několik technologií Intel®, jež mohou těmto potřebám vyjít vstříc, protože

- snižují riziko ztráty nebo odcizení citlivých informací
- chrání momentálně nevyužívané, přesouvané i právě používané citlivé informace
- chrání přístup k citlivým informacím pomocí silné autentizace
- umožňují lépe plnit kritéria politiky zabezpečení a ochrany osobních dat

Klíčová slova

Osobní informace, zdravotnický záznam, ochrana dat, bezpečnostní rizik, Intel Identity Protection Technology (IPT)

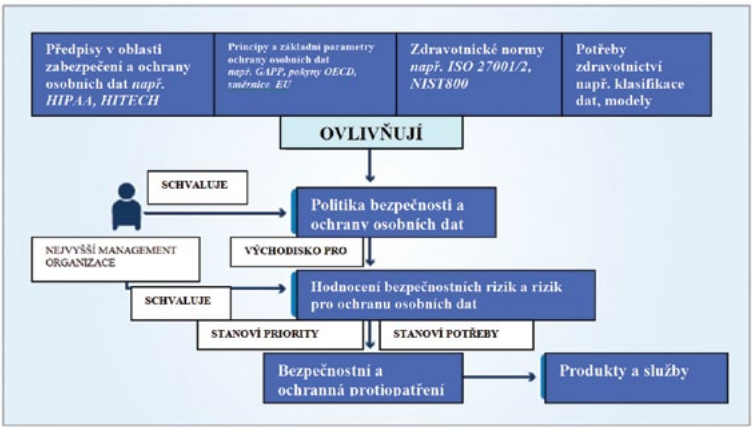
1. Identifikace potřeb v oblasti bezpečnosti a ochrany dat ve zdravotnických zařízeních

V dnešním světě životně důležitých elektronických informací a nebezpečných hrozeb zjišťují zdravotnická zařízení, že parametry zabezpečení a ochrany

dat definované na základě reaktivní, technologicky orientované metody směrem zdola nahoru neposkytují jim ani jejich pacientům dostatečnou ochranu. Zabránit prolomení ochrany citlivých informací a dalším typům bezpečnostních incidentů lze tehdy, pokud zdravotnická zařízení budou mít proaktivní, preventivní přístup s důrazem na budoucí potřeby zabezpečení a ochrany údajů. Chtějí-li zdravotnické organizace využít své omezené finanční prostředky způsobem, který maximální měrou sníží obchodní riziko, měly by zvolit postup shora dolů založený na hodnocení rizik a snížit riziko kombinací administrativních, fyzických a technických bezpečnostních mechanismů.

Jak ukazuje obr. 1, obecně uznávané známé metody stanovení potřeb v oblasti zabezpečení a ochrany osobních dat v určité organizaci se řídí příslušnými předpisy: normami pro bezpečnost řízení informačních systémů a způsoby zabezpečení[1], jako jsou ISO 27001 a ISO 27002 vydané Mezinárodní organizací pro normalizaci (International Standards Organization), a zásadami typu GAPP (Generally Accepted Privacy Principles, Obecně přijímané zásady ochrany osobních údajů)[2] vydanými Americkým institutem certifikovaných veřejných účetních (American Institute of CPA), dále pokyny Organizace pro hospodářskou spolupráci a rozvoj (OECD)[3] a směrnicemi Evropské unie.[4]

Dalším klíčovým faktorem ovlivňujícím bezpečnost a ochranu dat v rámci zdravotnické organizace jsou specifické požadavky zdravotnictví jako celku, k nimž patří klasifikace dat a modely použití. Základ zabezpečení a ochrany dat zdravotnické organizace tvoří koncepce, která by měla podléhat kontrole a schvalování nejvyššího vedení takové organizace.



Obrázek 1 — Identifikace požadavků na bezpečnost a ochranu osobních dat ve zdravotnickém zařízení

Hodnocení rizik týkající se bezpečnosti a ochrany osobních dat se provádí na základě stanovené koncepce a spočívá v modelování rizik. Riziko je funkcí pravděpodobnosti, že dojde ke zneužití slabého místa v systému zabezpečení,

a následného obchodního dopadu takového prolomení ochrany. Modelová rizika, která vzejdou z hodnocení, lze seřadit podle pravděpodobnosti vzniku a obchodního dopadu a porovnat s referenční mírou přípustného rizika stanovenou v rámci politiky. Rizika, která přesáhnou stanovenou úroveň, je pak možné snižovat v pořadí dle priorit pomocí protiopatření označovaných také jako bezpečnostní mechanismy nebo ochranná opatření. Zmírnění rizik podle pořadí priorit umožní zdravotnickému zařízení využít jeho omezený rozpočet ke snížení úrovně maximálního obchodního rizika.

Podle definice je bezpečnost a ochrana osobních údajů adekvátní, pokud se míra rizika pohybuje ve stanoveném přípustném intervalu. To umožňuje zdravotnickému zařízení přistupovat k problematice bezpečnosti a ochrany osobních dat přiměřeným způsobem a rozhodnout, kdy je úkol splněn. Protiopatření k zabezpečení a ochraně osobních údajů identifikovaná touto cestou lze implementovat pomocí bezpečnostních produktů a služeb. Společnost Intel poskytuje širokou škálu hardwarově podporovaných bezpečnostních technologií včetně následujících:

- Intel® AES–NI k ochraně důvěrnosti momentálně nevyužívaných, přesouvaných či právě používaných citlivých informací, s novými instrukcemi pro silné, vysoce výkonné šifrování vycházející z široce používané normy Advanced Encryption Standard5
- Intel® Anti–Theft Technology (Intel ® AT) pro snížení rizika ztráty nebo krádeže citlivých informacích v počítači6
- Intel® Identity Protection Technology (Intel ® IPT) se silnou autentizací chránící přístup k citlivým informacím; k dispozici ve vybraných počítačích s procesorem Intel® Core™ druhé generace7
- Intel® Virtualization Technology (Intel ® VT) zajišťující vysoký výkon a bezpečí při práci na počítači ve virtuálních prostředích využívaných v datových centrech, cloudových aplikacích nebo virtualizovaných počítačích8
- Intel® Trusted Execution Technology (Intel ® TXT) chránící důvěrnost a integritu dat v systémech zdravotní péče a citlivé informace v počítačích a na serverech9
- Intel® Active Management Technology (Intel ® AMT) pro bezpečnou vzdálenou správu počítačů; zlepšuje zabezpečení a ochranu osobních dat, jejich integritu a dostupnost, čímž přispívá k dodržování politiky bezpečnosti a ochrany osobních dat.

2. Ochrana důvěrnosti, integrity a dostupnosti

Potřeba ochrany osobních údajů a zamezení neoprávněnému přístupu k nim je ve zdravotnictví chápána relativně dobře. Tato nutnost je vedena snahou zabránit prolomení ochrany citlivých informací. Řada předpisů dnes ukládá povinnost takové prolomení oznámit, jeho důsledky jsou proto závažnější než kdykoli předtím. Účinným protiopatřením, které může pomoci chránit data před zcizením, je šifrování. Uživatelé ovšem mohou svůj šifrovací software vypínat z obavy, že jeho funkční požadavky zpomalí chod počítače a ovlivní tak použitelnost aplikace a produktivitu uživatele. Intel AES–NI nabízí hardwarově podporované šifrování, které dává

nemocničním lékařům do rukou zabezpečení prostřednictvím šifrování při současném zachování dobrého výkonu, použitelnosti a produktivity. V porovnání s výhradně softwarovým způsobem šifrování AES dokáže Intel AES–NI šifrování třikrát až desetkrát zrychlit.[10]

V oblasti zdravotní péče je třeba chránit důvěrnost citlivých informací v rozsahu end–to–end, ať už se data uchovávají, používají či vyměňují. Intel AES–NI představuje univerzální řešení využitelné ve zdravotnických zařízeních v různých situacích, kdy je potřeba šifrování – na rozdíl od jiných řešení urychlujících šifrování jen v jedné konkrétní oblasti jako např. samošifrovací disky nebo hardwarové akcelerátory Secure Sockets Layer/ Transport Layer Security (SSL/TLS).Intel AES–NI lze použít k zašifrování informací, jež spočívají na pevném disku nebo ve vyměnitelném paměťovém zařízení, přesouvají se (například pomocí protokolu SSL/TLS) nebo se používají v aplikacích a databázích. Tato všestrannost podporuje odolné end–to–end zabezpečení citlivých informací v celém zdravotnickém systému. Ve zdravotnictví je nutné chránit citlivá data v rozsahu end–to–end, ať už jsou uložená nebo se právě používají či přesouvají.

V oblasti zdravotní péče je třeba chránit důvěrnost citlivých informací v rozsahu end–to–end, ať už se data uchovávají, používají či vyměňují.

S tím, jak se v systémech podnikových zdravotních záznamů (Enterprise Health Record–EHR) soustřeďuje stále více citlivých informací, stává se požadavek zamezit prolomení ochrany prostřednictvím neoprávněného přístupu do EHR zásadním. Ověření typu „co víte" pomocí uživatelského jména/hesla je relativně slabé. Zvyšování složitosti hesel má v praxi omezený úspěch, s rostoucí složitostí hesla se totiž zvyšuje pravděpodobnost, že si je uživatelé napíšou nebo zapomenou, a pak zatěžují help desk.

Koncepce zdravotnického zařízení je východiskem pro metody zabezpečení a ochrany dat.

Navíc i silná a složitá hesla jsou náchylná k malwaru, jako jsou např. key loggery. Dvoufaktorová autentizace typu „máte u sebe" s využitím hardwarových tokenů sice zajišťuje silnou autentizaci, zároveň však přináší problémy v oblasti podpory a použitelnosti v případě ztráty či poškození šifrovacího tokenu nebo zatěžuje uživatele. Intel IPT nabízí silnou dvoufaktorovou autentizaci typu „co víte a máte", aniž by docházelo k potížím s podporou či použitelností. Kombinuje klasické heslo typu „co víte" s šestičíselným jednorázovým heslem spojeným s klientovou počítačovou platformou. Zdravotnická zařízení digitalizují životně důležitá data, a neméně důležitá je tudíž i ochrana integrity citlivých informací a systémů, které je zpracovávají.

To znamená zajistit jednak celistvost, přesnost a aktuálnost citlivých informací a systémů a jednak to, aby změny v nich prováděly pouze osoby k tomu oprávněné. Intel TXT poskytuje důvěryhodné prostředí pro spouštění zdravotnických aplikací obsahujících citlivá data. Toto prostředí disponuje funkcí ověřeného spuštění, která zajišťuje integritu pracovního prostředí, jakým je např. virtuální stroj (VM), a snižuje rizika spojená s přítomností malwaru nebo rootkitů. Intel TXT umožňuje také hardwarově řízenou separaci

jednotlivých VM, čímž chrání integritu a důvěrnost zdravotnických aplikací s citlivými daty spuštěných na souběžně provozovaných VM před malwarem.

Dojde–li k vypnutí VM se spuštěnou zdravotnickou aplikací, dokáže Intel TXT vyčistit paměť a ochránit tak důvěrnost v ní uložených citlivých informací. Nástroje pro zabezpečení v rámci aplikace Intel TXT hrají obzvláště důležitou roli ve sdíleném virtualizovaném prostředí, jakým je např. prostředí cloudové. Ve virtualizovaném prostředí Intel VT rovněž zajišťuje zvláštní ochranu grafiky a I/O (vstupů a výstupů). Intel TXT využívá hardwarový modul Trusted Platform Module (TPM), který nabízí také hermeticky uzavřené úložiště střežící uložená i právě používaná citlivá data před útokem. Tato funkce může přispět k ochraně certifikátů sloužících k ověření identity lékaře. Péče o pacienta se stává kriticky závislou na elektronických záznamech o pacientech a pracovních tocích, proto musejí být zdravotnická zařízení s to zajistit oprávněným osobám přístup k citlivým informacím kdykoli je třeba. Včasný a spolehlivý přístup k datům tak nabývá stejného významu jako ochrana důvěrnosti a integrity těchto dat. Z hlediska dostupnosti čelí zdravotnická zařízení řadě hrozeb. Některé z nich jsou úmyslné jako např. útoky vyvolávající odepření služby, některé náhodné či způsobené prostředím. Odolné, holisticky koncipované zabezpečení a ochrana osobních dat mohou tato rizika snížit pomocí protiopatření, jakými jsou systémy detekce a prevence napadení, zálohování a obnova dat, plán zajištění kontinuity činnosti a plán obnovy po mimořádné události.

3. Odolné vícevrstvé zabezpečení

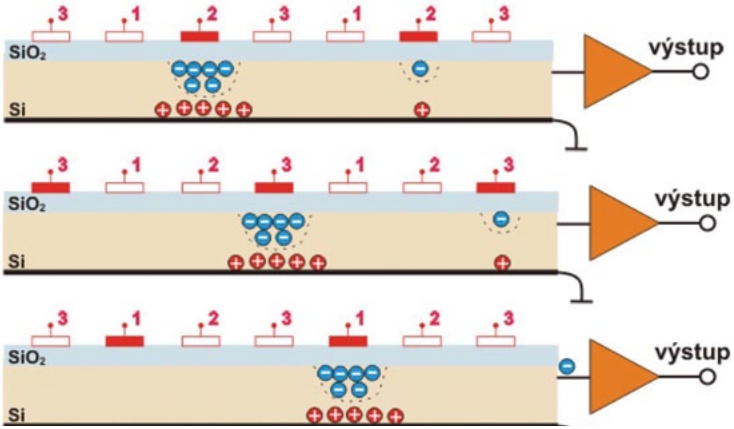
Snížení rizika a zajištění odolného zabezpečení a ochrany osobních údajů v rámci zdravotnického zařízení vyžaduje administrativní, fyzické i technické bezpečnostní mechanismy (viz obr. 2). Pro ilustraci: pouhé technické zabezpečení pomocí šifrování nedosahuje v praxi takového účinku, jako když je spojeno s administrativními mechanismy, jakými jsou např. politika kladoucí důraz na zachování důvěrnosti citlivých informací, školení v oblasti zabezpečení a dohled nad prosazováním takové koncepce. K zajištění bezpečného používání, přesouvání a uchovávání zařízení obsahujících a zpracovávajících citlivé informace jsou rovněž nutné fyzické bezpečnostní mechanismy jako např. zámky či zabezpečení perimetru.

4. Odolné a výkonné hardwarově podporované zabezpečení

V porovnání s čistě softwarovými typy technických bezpečnostních mechanismů potřebných ke snížení bezpečnostních rizik a rizik týkajících se ochrany osobních dat nabízí hardwarově podporované zabezpečení – kombinované s kompatibilním softwarem – zásadní výhody. Útoky na zdravotnické organizace a systémy jsou stále rafinovanější. Tradiční výhradně softwarové bezpečnostní mechanismy lze obejít a mohou podléhat virovým útokům. Hardwarově podporované zabezpečení může tyto systémy ve zdravotnické organizaci upevnit (obr. 3). Ústřední důvěryhodný hardwarový prvek jako základ bezpečnostního řešení je na rozdíl od výhradně softwarových řešení stálý a nepodléhá

virovým útokům. Tuto odolnost lze převést na vyšší prvky zabezpečení např. prostřednictvím ověřeného spuštění nebo stupňovitého bootovacího řetězce, kterým disponuje aplikace Intel TXT.

Ze zkušenosti víme, že hardwarově podporované zabezpečení je také lépe přijímáno, protože odpadá riziko snížení výkonu, což možná v minulosti vedlo řadu uživatelů k vypínání softwarového zabezpečení. Zvýšená složitost znamená vyšší zranitelnost. Hardwarově podporované zabezpečení přesouvá základní procesy do hardwaru, kde jsou méně náchylné k narušení, např. k únikům vedlejším kanálem. To také zjednodušuje a zefektivňuje softwarovou část bezpečnostního řešení, protože snižuje jeho zranitelnost a zvyšuje odolnost celého bezpečnostního řešení. Výhody hardwarově podporovaného zabezpečení se ve finálním bezpečnostním řešení projeví jen tehdy, jestliže je software a služby ve vyšších úrovních řešení s to rozpoznat toto hardwarově podporované zabezpečení a jsou-li s ním kompatibilní. K aktivaci hardwarově podporovaného zabezpečení je také obvykle nutné nastavení a konfigurace.



Obrázek 2 — Vícevrstvá metoda zabezpečení a ochrany osobních dat

Bezpečnostní technologie Intel nabízejí odolné, vysoce výkonné hardwarově podporované nástroje pro vyšší bezpečnost. Tyto technologie se maximální měrou opírají o normy: např. AES–NI vychází z normy Advanced Encryption Standard standardizované Národním institutem pro normalizaci a technologie (National Institute of Standards and Technology, NIST)11 a momentálně je nejrozšířenější symetrickou blokovou šifrou. Tyto hardwarově podporované technologie také představují otevřenou platformu pro třetí strany (dodavatele softwaru a poskytovatele služeb), které mohou inovovat a poskytovat kompatibilní software a služby.

Bezpečnostní technologie Intel poskytují odolné a vysoce výkonné hardwarově podporované nástroje pro vyšší bezpečnost.

Obrázek 4 — Hardwarově podporované zabezpečení

5. Posílení bezpečnosti pomocí hloubkové ochrany

Šifrování samozřejmě není všelékem proti prolomení ochrany. Tento typ bezpečnostní ochrany může selhat, pokud uživatel šifrování vypne, používá slabá šifrovací hesla nebo ponechá systém nezamčený (např. ponechá laptop aktivní nebo v pohotovostním režimu, který nevyžaduje předbootovací autentizaci). Takové kroky otvírají dveře závažným a finančně nákladným útokům, řada zdravotnických zařízení proto žádá vyšší úroveň zajištění bezpečnosti citlivých informací. Toho lze dosáhnout pomocí vícevrstvé hloubkové ochrany.

Technologie Intel Anti-Theft může dále snížit riziko ztráty nebo krádeže citlivých informací z notebooku. V případě ztráty či odcizení notebooku do něj může zdravotnická organizace poslat „jedovatou pilulku". Ta počítači zabrání v nabootování a v přístupu k citlivým informacím, čímž se sníží riziko narušení důvěrnosti citlivých informací. Pokud je ztracený nebo odcizený notebook nedostupný přes síť, lze ochranu Intel AT spustit lokálně pomocí hardwarového časovače, který se zapíná, pokud notebook kontaktuje centrální server se zpožděním. Podobně se může zabezpečení Intel AT lokálně zapnout na notebooku tehdy, když počet opakovaných neúspěšných pokusů o přihlášení dosáhne stanoveného maxima. Intel AT představuje další vrstvu odolné ochrany nad úrovní šifrování. Tyto dvě vrstvy technického bezpečnostního mechanismu společně poskytují hloubkovou ochranu citlivým informacím v přenosných počítačích a tím i větší jistotu zdravotnickým zařízením a pacientům, že jsou jejich data v bezpečí.

6. Snižování rizik v průběhu životního cyklu hrozby

Ke snížení bezpečnostních rizik a rizik souvisejících s ochranou osobních dat ve zdravotnických zařízeních je třeba podnikat kroky v celém životním cyklu

hrozeb, od prevence, přes detekci, reakci až po obnovu dat. Hlavním cílem politiky bezpečnosti a ochrany citlivých údajů ve zdravotnických zařízeních je nepřetržitá aktualizace systému. Neustále vyvstávají nová slabá místa, a to zejména v oblasti softwaru. Snížení rizika výskytu bezpečnostních incidentů spojených s těmito novými slabými místy vyžaduje včasnou aplikaci aktualizačních bezpečnostních záplat. Pokud je slabé místo zjištěno až na základě zero-day útoku, dodavatelé softwaru vyvinou a vydají opravnou záplatu. Zdravotnické zařízení pak musí tuto záplatu zavést co nejdříve do svých počítačů, protože každé zpoždění zvětšuje prostor pro útok vedený proti takovému nově zjištěnému slabému místu.

Zabezpečovací technologie Intel představují odolné, vysoce výkonné hardwarově podporované nástroje k posílení ochrany.

Opravné záplaty lze obvykle rozšířit k většině počítačů v rámci jedné skupiny automaticky a včas. Není však výjimkou, že záplatování selže až u 20 procent počítačů takové skupiny např. proto, že jsou vypnuté nebo nefunkční. Každé prodlení s aplikací bezpečnostní záplaty zvětšuje prostor pro útok proti nově zjištěnému slabému místu a zvyšuje riziko bezpečnostních incidentů.

Počítač vybavený procesorem řady Intel® Core™ vPro™ umožňuje vzdálenému centrálnímu administrátorovi zabezpečené připojení a instalaci opravné záplaty prostřednictvím kabelové nebo bezdrátové sítě, a to i v případě, že je počítač vypnutý.12 To umožňuje počítačovým technikům rychleji a efektivněji rozšiřovat opravné záplaty do všech počítačů, čímž brání vzniku nákladů a zpoždění spojených s jejich fyzickou návštěvou pracovišť. Zmenšením prostoru pro případný útok na nově zjištěné slabé místo se rovněž snižují rizika. Taková aplikace technologie Intel ® vPro ™ je příkladem technického bezpečnostního mechanismu používaného v preventivní fázi životního cyklu hrozby. Technologii Intel vPro je možné použít i v případě, kdy je počítač už nakažený malwarem, a to k rychlejšímu a efektivnějšímu řešení problému ve fázi obnovy dat, bez nákladného a časově náročného zásahu technika na pracovišti. Tato technologie umožňuje lékaři rychlý návrat k práci na jeho počítači a zároveň zvyšuje produktivitu a snižuje náklady na IT podporu.

7. Šest kroků k dokonalejšímu zabezpečení a ochraně osobních dat ve zdravotnictví

Bezpečnostním incidentům, jakým je např. prolomení ochrany, se lze vyhnout, vyžaduje to ovšem dlouhodobý proaktivní a preventivní přístup tj. aby zabezpečení a ochrana osobních údajů, hodnocení rizik a protiopatření byla na svém místě dříve, než se hrozba objeví. Budování bezpečnostních a ochranných nástrojů ve vaší organizaci je postupný, opakovaný a nepřetržitý proces. Začněte ihned a postupujte následujícím způsobem:

1. Vybudujte systém zabezpečení a ochrany osobních dat ve své zdravotnické organizaci podle standardního schématu shora dolů.
2. Stanovte a vytvořte vlastní politiku bezpečnosti a ochrany osobních dat,

přičemž do ní integrujte příslušné předpisy, zásady ochrany osobních údajů, normy a vlastní potřeby v oblasti kategorizace dat, praktických modelů a zpracování dat. Definujte požadavky na zabezpečení a ochranu osobních údajů během jejich sběru, používání, uchovávání, zveřejňování a skartování.

3. Zvolte zabezpečení a ochranu osobních dat založenou na hodnocení rizik. To vám umožní vybudovat optimálně zaměřený a účelný systém, který maximální měrou zužitkuje váš omezený rozpočet a co nejvíce sníží obchodní rizika.
4. Snižte riziko narušení a dalších bezpečnostních incidentů pomocí odolné vícevrstvé hloubkové ochrany, která pokryje celý životní cyklus hrozby.
5. Použijte hardwarově podporované bezpečnostní technologie Intel, zlepšíte tím odolnost a výkonnost vašich technických bezpečnostních mechanismů.
6. Maximalizujte hodnotu vašich bezpečnostních mechanismů holistickým způsobem, který zajistí, že bezpečnostní mechanismy na úrovni hardwaru, softwaru i služeb budou kompatibilní a budou fungovat harmonicky, čímž maximální měrou sníží obchodní riziko.

Počítač vybavený procesorem řady Intel® Core™ vPro™ umožňuje vzdálenému centrálnímu administrátorovi zabezpečené připojení a instalaci opravné záplaty prostřednictvím kabelové nebo bezdrátové sítě, a to i v případě, že je počítač vypnutý.

Další krok:

Kontaktujte svého obchodního zástupce společnosti Intel nebo navštivte internetové stránky Intelu věnované informačním technologiím ve zdravotnictví:

Více informací o zabezpečovacích technologiích Intel k dispozici na:

- *www.intel.com/technology/anti–theft*
- *www.intel.com/technology/dataprotection*
- *www.intel.com/technology/identityprotectiontechnology*
- *www.intel.com/technology/malwarereduction*
- *www.intel.com/technology/virtualization/technology.htm*
- *www.intel.com/technology/vpro/*

Poznámky:

[1.] http://www.iso.org

[2.] http://www.aicpa.org

[3.] http://www.oecd.org

[4.] http://eur–lex.europa.eu

[5.] AES–NI je sada instrukcí, která kombinuje matematické operace použité v algoritmu Advanced Encryption Standard (AES). Technologie AES–NI vyžaduje jednak to, aby byl počítačový systém vybaven procesorem podporujícím instrukce AES–NI a jednak aby software od jiných dodavatelů než Intel byl schopen vykonávat tyto instrukce ve správném pořadí. AES–NI je k dispozici v procesorech řad Intel ® Core ™ i5–600 Desktop Processor,

Intel ® Core ™ i7–600 Mobil Processor a Intel ® Core ™ i5–500 Mobil Processor. Pro informace o dalších procesorech a systémech podporujících technologii AES–NI se obraťte na vašeho prodejce nebo výrobce systému. Více informací na http://softwarecommunity.intel.com/isn/downloads/intelavx/AES–Instructions–Set_WP.pdf.

[6.] Žádný počítačový systém nemůže zajistit absolutní bezpečnost za všech okolností. Technologie Intel ® Anti–Theft (Intel ® AT) vyžaduje, aby čipset, BIOS, verze firmwaru, software daného počítače podporovaly aplikaci Intel AT a aby technologie poskytovatele služeb připojení a nezávislého dodavatele softwaru (independent software vendor–ISV) byly kompatibilní s aplikací Intel AT. Veškeré detekční (triggery), reaktivní (akce) a obnovovací mechanismy fungují teprve až po aktivaci a konfiguraci funkce Intel AT. Určité funkce nemusejí být v nabídce všech ISV či poskytovatelů služeb a rovněž nemusejí být dostupné ve všech zemích. Intel nenese žádnou odpovědnost za ztrátu či odcizení dat a/nebo systémů nebo jakékoli jiné škody vzniklé v důsledku takové ztráty či odcizení.

[7.] Žádný počítačový systém nemůže zajistit absolutní bezpečnost za všech okolností. Intel IPT vyžaduje čipset, BIOS, firmware a software s podporou této technologie a internetové stránky, které využívají řešení Intel® IPT od autorizovaného poskytovatele služeb Intel® IPT. Poraďte se s výrobcem vašeho systému nebo vaším poskytovatelem služeb o dostupnosti a funkcích. Intel nenese žádnou odpovědnost za ztrátu či odcizení dat a/nebo systémů nebo jakékoli jiné škody vzniklé v důsledku takové ztráty či odcizení.

[8.] Technologie Intel ® Virtualization vyžaduje počítačový systém s procesorem Intel ®, BIOSem, virtuálním strojovým monitorem (VMM) podporujícími tuto technologii a pro některé účely také určitý software s ní kompatibilní. Funkčnost, výkon a jiné výhody se mohou lišit v závislosti na konfiguraci hardwaru a softwaru a mohou případně požadovat aktualizaci systému BIOS. Softwarové aplikace nemusejí být kompatibilní se všemi operačními systémy. Kompatibilitu, prosím, konzultujte se svým dodavatelem aplikace,.

[9.] Žádný počítačový systém nemůže zajistit absolutní bezpečnost za všech okolností. Intel Trusted Execution Technology (TXT) je bezpečnostní technologie, která ke svému provozu potřebuje počítačový systém s technologií Intel ® Virtualization, procesor Intel s technologií Intel Trusted Execution Technology, čipset, BIOS, moduly Authenticated Code Modules a virtuální strojový monitor Intel nebo jiný kompatibilní s technologií Intel ® Trusted Execution Technology. Kromě toho technologie Intel Trusted Execution Technology vyžaduje, aby byl systém vybaven aplikací TPM v1.2, jak požaduje Trusted Computing Group, a pro některé účely také specifickým softwarem. Více informací na http://www.intel.com/.

[10.] Stáhněte si článek o mimořádně výkonné technologii Intel AES s novými instrukcemi z http://software.intel.com/en–us/articles/intel–advanced–encryption–standard–instructions–aes–ni/

[11.] Publikace FIPS 197, http://csrc.nist.gov/publications/fips/fips197/fips–197.pdf

[12.] Intel ® vPro ™ obsahuje výkonnou technologii Intel ® Active Management Technology (Intel ® AMT). Intel AMT vyžaduje, aby byl počítač vybaven čipsetem s podporou technologie Intel® AMT, síťovým hardwarem, softwarem, a dále také připojením ke zdroji napájení a podnikové síti. Zákazník musí konfigurovat nastavení, které může k aktivaci některých funkcí vyžadovat rovněž skriptování v konzoli pro správu nebo další integraci do stávajících bezpečnostních rámců či úpravy nebo implementaci nových podnikových procesů. Pro notebooky nemusí být technologie Intel AMT dostupná nebo mohou být některé její funkce omezeny podle konkrétní implementace virtuální privátní sítě využívané pod instalovaným operačním systémem (OS) nebo při bezdrátovém připojení, při bateriovém napájení, v režimu spánku či hibernace nebo je–li počítač vypnutý. Více informací na http://www.intel.com/technology/platform–technology/intel–amt/.

Informace obsažené v tomto dokumentu jsou poskytovány v souvislosti s produkty Intel ®. Tento dokument neuděluje žádnou licenci k právům a duševnímu vlastnictví, ať už výslovnou nebo implicitní, vzniklou na základě právní překážky nebo jinak. S výjimkami uvedenými v obchodních podmínkách společnosti Intel® pro určité produkty nenese Intel žádnou odpovědnost a Intel nepřebírá žádné výslovné či implikované záruky týkající se prodeje a/nebo používání produktů Intel včetně odpovědnosti či záruk v souvislosti s vhodností pro určitý účel, obchodovatelností nebo porušením jakéhokoli patentu, autorských práv či jiných práv k duševnímu vlastnictví. Pokud Intel výslovně písemně nesjedná jinak, nejsou produkty Intel navrženy ani určeny pro žádné použití, při němž by selháním produktu Intel vznikla situace, v níž by mohlo dojít ke zranění nebo smrti osoby.

Intel může provádět změny specifikací a popisy produktů kdykoli, bez předchozího upozornění. Návrháři se nesmějí opírat o neuvedené charakteristiky nebo charakteristiky jakýchkoli vlastností či instrukcí s označením „vyhrazené" nebo „nedefinované". Intel je bude definovat v budoucnu a nenese žádnou odpovědnost za rozpory nebo nekompatibilitu plynoucí z takových v budoucnu provedených změn. Zde uvedené informace se mohou měnit bez předchozího upozornění, nejsou určeny pro finální návrh. Produkty popsané v tomto dokumentu mohou obsahovat konstrukční vady nebo chyby označované jako errata, jež mohou způsobit odchylku produktu od uveřejněné specifikace. Momentálně specifikovaná errata jsou k dispozici na vyžádání. Než si objednáte zboží, kontaktujte místní pobočku Intelu nebo svého distributora, kde také můžete získat nejnovější specifikace. Kopie dokumentů s pořadovým číslem, na něž tento dokument odkazuje, nebo jiné dokumenty Intelu je možné získat na telefonním čísle 1–800–548–4725 nebo na adrese webových stránek Intel na www.intel.com.

Copyright © 2011 Intel Corporation. Všechna práva vyhrazena. Intel, logo Intel, Intel Xeon, Intel Core a Intel vPro jsou ochranné známky společnosti Intel Corporation ve Spojených státech a dalších zemích.

Další jména a značky mohou být majetkem jiných subjektů.

Kontakt:

MUDr. Pavel Kubů
email: *pavel.kubu@intel.com*