Ovlivnění kybernetické bezpečnosti pandemií COVID-19

Pavel Zapletal

Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky

Nad Stráněmi 4511, 760 05 Zlín

p2_zapletal@utb.cz

Abstrakt: Tento článek se zabývá kybernetickou bezpečností v době šíření nemoci COVID-19. Podniky musely změnit koncept pracovní náplně svých zaměstnanců. Přechod na home office přinesl nové hrozby pro podnik. Nenadálé situace využili útočníci, kteří mimo jiné zaútočili i nemocnice v rámci ČR.

Klíčová slova: COVID-19, home office, kybernetický útok, ransomware, vishing

ÚVOD

Doba covidová přinesla změny v podnicích a institucích, které přetrvají v plné míře nebo částečně i po odeznění nemoci COVID-19 a jejích stále nových mutací. Jedná se zejména o místo výkonu svého povolání a způsobu komunikace se spolupracovníky a vedoucími pracovníky organizací. V době „předcovidové“ bylo pro většinu podniků zabývajících se kancelářskou prací, standardem pracovat na jednom pracovišti. Na místě se od pondělí do pátku scházel nižší, střední i top management s pevnou pracovní dobou. V podstatě ze dne na den došlo k razantní změně z důvodu nárůstu nemocných osob virem COVID-19. Mnoho podniků se rozhodlo, že jejich zaměstnanci začnou vykonávat pracovní povinnosti ze svých domovů.

Home office a kybernetická bezpečnost

Jedná se o pracovní činnost, která není vykonávána na standardním místě zaměstnavatele, ale přímo v domácnosti jednotlivých zaměstnanců. Home office není samozřejmě vhodný pro povolání řemeslná a jiná, která jsou svou podstatou závislá na konkrétním prostředí. Týká se to především osob, jejichž činnost je nebo spíše byla vykonávána v kancelářských

budovách s pomocí počítačů. Přesun činnosti zaměstnanců do jejich domovů měl pozitivní vliv na menší pravděpodobnost onemocnění většího množství pracovníků jednotlivých organizací nemocí COVID-19, jelikož nedochází k tak častému setkávání se osob na jednom místě, ale i po cestě do zaměstnání. S tím je úzce spjata schopnost organizace vykonávat nadále svou činnost, i když v omezeném množství od začátku vypuknutí nemoci v rámci ČR a také celého světa.

Podniky postupně začaly zjišťovat, že při práci jejich zaměstnanců z domova zanikají výrazné měsíční náklady spojené s pronájmem kancelářských komplexů, kdy dané finanční prostředky lze využít na něco jiného. Vynucená změna pracovního prostředí měla pozitivní vliv také pro přírodu a další oblasti života na zemi. Všechno má své kladné i záporné stránky. V případě home office byla zásadně negativní stránkou nepřipravenost podniků na možnost poněkud rychlého přesunu výkonu pracovních činností do domácností zaměstnanců. Mimo podniky, jejichž činnost musela být úplně pozastavena, začala být u ostatních podniků nejvíce ohrožena jejich bezpečnost z oblasti kybernetického zabezpečení. I když mohla být kvalitně zabezpečena firemní elektronické zařízení v podniku, nejslabším článkem podniků se stala elektronická zařízení využívaná zaměstnanci k pracovním činnostem v jejich domácnosti. Doba „covidová“ je rájem pro útočníky a hackery, kteří si za cíl vyberou některý z obdobných podniků.

Podle stanovených cílů útočníků se může jednat o kybernetický útok na popsaný podnik, který je veden na počítač zaměstnance formou DDoS útoku, útokem na přihlašovací heslo počítače zaměstnance, phishingovým útokem, útokem ransomwaru a jiné.

DDoS útoky spočívají v odepření služby na základě zahlcení počítačového systému oběti velkým množstvím požadavků. Jedná se o cílený útok, který prostřednictvím botnetu otevírá spojení nebo uskutečňuje dotazy na webovou stránku či server. Výsledkem je zpomalení systému oběti anebo přímo jeho zhroucení. [1]

Phishing je útokem řadícím se mezi sociální inženýrství. Cílem phisingu je získání finančních prostředků pachatelem od své oběti na základě získání důvěry oběti a jejího následného oklamání.

Kromě standardních phishingových útoků přes emailové schránky se rozšířil i Vishing. Vishingový útok se od phishingového útoku liší jeho provedením. Na místo elektronické komunikace je prováděn prostřednictvím telefonního hovoru. Pachatelé se nejčastěji představují jako pracovníci některé z bank, s tím, že zjistili neoprávněný přístup k bankovnímu

účtu volaného. Snahou pachatele je osobu vystrašit, osobě je doporučeno, aby ihned přesunula své finanční prostředky ze současného bankovního účtu na bankovní účet sdělený pachatelem během telefonního hovoru. Pachatel v telefonátu slibuje, že peníze budou volanému vráceny ihned po vyřešení problému. Oběť tedy své finanční prostředky přesune na uvedený bankovní účet a většinou své peníze již nikdy neuvidí. Jedinou šancí je oznámení skutečnosti policejnímu orgánu, který je jedinou nadějí případného dohledání pachatele a přes soudní řízení vrácení peněžních prostředků oběti. Poškozenou stranou tímto jednáním může být fyzická osoba, ale také právnická osoba. [2]

Ransomware je softwarem, který slouží k zašifrování dat oběti a následně od své oběti požaduje výkupné za dešifrování jejich dat. [3]

Kybernetické útoky ransomwarem mohou podnikům způsobit následující nepříjemnosti:

a) náklady na prostoje,
b) náklady v souvislosti s dvojím vydíráním,
c) náklady spojené se zaplacením výkupného,
d) náklady na zvýšení IT zabezpečení,
e) náklady spojené s poškozením značky.

Náklady na prostoje bývají zásadní položkou pro napadený podnik. Poškozenému podniku obvykle nějakou dobu trvá, než se mu podaří obnovit systémy po útoku. S rostoucí prodlevou obnovy systémů rostou samotné škody pro podnik. Škoda je nejčastěji tvořena ze ztráty příležitostí pro podnik, poklesu oblíbenosti u svých zákazníků, poškození značky podniku, nemožnosti plnění dohodnutých obchodních spoluprací, regulační pokuty, právní výdaje a jiné. Náklady způsobené prostoji bývají často výrazně vyšší než náklady na výkupné.

Náklady v souvislosti s dvojím vydíráním tvoří dvě části. Útočníci nejprve po napadení odcizí velkého množství dat a teprve následně provedou zašifrování dat podniku. Druhá část útoku je tvořena vydíráním podniku ohledně zaplacení výkupného pro dešifrování dat. V případě nezaplacení požadované částky útočníci zveřejní odcizená data do prostředí dark webu.

Náklady spojené se zaplacením výkupného mohou být výrazně vyšší než náklady pro zajištění obnovy systémů a ještě s nejistým výsledkem dešifrování dat. Podnik by měl zvážit a porovnat hodnotu nákladů na výkupné s náklady na obnovu bez zaplacení výkupného. V potaz je třeba brát také možnost, že po zaplacení výkupného se poškozený podnik ke svým datům stejně nedostane.

Náklady spojené se zvýšením IT zabezpečení napadeného podniku většinou často následují po provedeném kybernetickém útoku. Cílem podniku je zajistit takové IT zabezpečení, které by předešlo možným opakovaným útokům na podnik a z toho plynoucích následků. Zaplacení výkupného útočníkům nemusí vést k dešifrování dat. Útočníci nemají žádnou motivaci pro dešifrování dat po zaplacení výkupného. Získané přístupy mohou být v danou dobu již dávnou prodány jiné skupině útočníků. Útočníci mohli také provést infikaci systémů prostřednictvím malwaru, takže ani zpřístupnění zašifrovaných dat nemusí být úplně bezpečné pro poškozený podnik.

Způsobené náklady v souvislosti s poškozením značky podniku mohou ovlivnit oblíbenost u svých zákazníků a jejich případný odliv ke konkurenčním společnostem s lepší reputací.

Video konference lze zahrnout mezi další rizikové oblasti. S omezením pohybu osob v rámci svých zemí i mimo ně se firemní meetingy a konference organizací přesunuly do online světa. Nedostatečná bezpečnostní opatření mohou přivodit velké nepříjemnosti, kdy může podnikovou poradu zachytit pracovník konkurenční společnosti, anebo se neveřejné informace z video konference mohou dozvědět neoprávněné osoby. Při neopatrnosti pozvaných osob k video konferenci a jejich neznalosti bezpečnostních zásad vznikají možnosti pro osoby znalé k jejich zneužití. Své o tom ví nizozemská ministryně obrany Ank Bijleveldová, která na sociální síť Twitter sdílela fotografii s přihlašovací adresou a pěti znaky pin kódu tvořícího šesti číslicemi. Po opakovaných pokusech zadání přihlašovacího hesla se nizozemskému novináři Danieli Verlaanu ze zpravodajské stanice RTL Nieuws skutečně podařilo připojit k video konferenci ministrů obrany Evropské unie. Naštěstí se po připojení do video konference ihned ukázal obraz z kamery přihlášeného novináře, takže připojení členové z konference zpozornili a novinář byl upozorněn, aby opustil konferenci. Novinář se následně skutečně odpojil z video konference. Ministryně obrany Nizozemska se přes svou mluvčí omluvila za chybu. Celé nedopatření poukazuje na jednu ze situací, které mohou nastat. [4]

Kybernetické útoky na nemocnice

Nedostatečná připravenost a samotného zabezpečení počítačových systémů se projevilo v řadě nemocnic na území České republiky.

Kybernetický útok na nemocnici v Benešově

Jednou z napadených nemocnic byla nemocnice Rudolfa a Stefanie v Benešově. Kybernetický útok na nemocnici v Benešově se uskutečnil dne 11. prosince 2019 pomocí malwaru Emotet a následného použití vyděračského počítačového viru Ryuk. Ransomware Ryuk útočí cíleně na vybrané subjekty. Subjekt, jehož počítačový systém je infikovaný virem Ryuk z počátku nemusí vědět o proniknutí viru do počítače. Vir nejprve prozkoumá veškerá přístupná data v napadeném počítači a teprve po hloubkové analýze provede jeho zašifrování. Ryuk umí po napadení počítače zajistit vypnutí antivirových programů. Oběť útoku je ze strany ruské skupiny stojící za ransomware Ryuk pouze informována o napadení virem Ryuk s uvedením kontaktní emailové schránky provozované na ProtonMailu pro následné vyjednávání o výkupném. Email je šifrován pomocí end-to-end šifrování bránící ztotožnění pachatelů útoku. Pomocí dostupných technologií není téměř možné provést dešifrování napadeného počítače, jelikož klíč k dešifrování mají pouze ruští útočníci. Útok s největší pravděpodobností započal hromadnou phisingovou a spamovou kampaní. Podvodný email obsahoval přílohu s fiktivní fakturou. Faktura vypadala jako by byla od věrohodného odesílatele, ale po jejím otevření došlo ke spuštění viru Emotet. Virus se přes skript dostal do veškerých počítačů, serverů a zařízení v síti. Následujícím krokem viru bylo stažení dalšího viru s názvem Trickbot z cloudu. Úlohou Trickbotu je zmapování všech hesel a jejich následné prolomení, včetně administrátorských. Po splnění svého úkolu nastoupil na řadu ransomware Ryuk s kódováním veškerých dat, což sebou neslo zpomalení sítě. Uživatelé telefonicky zkontaktovali pracovníky IT, kteří o tom vyrozuměli příslušné manažery a provedli odpojení všech počítačů. Nemocnice byla mimo provoz po dobu dvaceti dnů. Benešovské nemocnici byl znemožněn přístup do objednávek dárců krve, odcizena byla administrativní a ekonomická data. Ztráta se projevila zejména na základě omezení lékařských úkonů, kdy nemocnici nebyla proplacena naplánovaná vyšetření, operace a zákroky pacientů od zdravotních pojišťoven. Náklady byly vynaloženy také na pomoc externích pracovníků a nemocnice si za dva miliony korun zakoupila nový firewall. Podle tiskové mluvčí Policie ČR údajně nemělo dojít k úniků dat o složkách pacientů. Celková škoda způsobená nemocnici v Benešově byla vyčíslena na částku přesahující 59 milionů korun. Policejní orgán prověřované oznámení ukončil odložením věci podle § 159a trestního řádu, kdy se nepodařilo ztotožnit osobu či osoby pachatelů. V lednu roku 2021 vydal Národní úřad pro kybernetickou a informační bezpečnost oficiální prohlášení, že se podařilo rozkrýt a eliminovat infrastrukturu, kterou používali pachatelé pro šíření malwaru

Emotet. Po celém světě byly stovky serverů tvořících infrastrukturu malwaru Emotet. Na samotném rozkrytí pracoval Eurojust, Europol a policejní orgány z Kanady, Nizozemska, Ukrajiny, Spojených států, Spojeného království, Francie a Německa. [5],[6],[7],[8]

Kybernetický útok na nemocnici v Brně

Dne 13. března 2020 byl proveden kybernetický útok na Fakultní nemocnici v Brně v Bohunicích. Útočníkům se podařilo znepřístupnit internetový objednávací systém nemocnice sloužící dárcům krve pro jejich objednání. Nemocnice musela přijít na objednávání prostřednictvím telefonických hovorů. Nemocnice mimo jiné ztratila přístup k některým z administrativních a ekonomických dat. Veškeré plánované operace v nemocnici byly odloženy. Akutní pacienti byli převezeni do jiných nemocnic v rámci jihomoravského kraje. Útok na Fakultní nemocnici v Brně ovlivnil také další nemocnice. Například Fakultní nemocnice u svaté Anny v Brně nebo nemocnice v Kyjově musely rušit naplánované operace. Jaroslav Štěrba, jako ředitel Fakultní nemocnice k situaci ohledně kybernetického útoku uvedl, že po útoku nebylo možné přenášet informace z jednotlivých laboratoří do databázového systému. Vyšetření pacientů trvalo oproti standardnímu stavu o něco déle. Jedním z důvodů byla například nutnost přejít na ruční vypisování receptů nebo psaní na psacích strojích. Nemocnice nepřišla o data týkající se pacientů. Napadené nemocnici se povedlo obnovit i historii emailové komunikace. [9],[10]

Odvrácené kybernetické útoky nemocnic

Neúspěšný pokus o kybernetický útok byl také proveden na Fakultní nemocnici Ostrava dne 16. dubna 2020. O několik dní dříve se nemocnici podařilo odrazit i phishingový útok. Ve stejném období Fakultní nemocnice Olomouc zaregistrovala podezřelé aktivity spojené se zvýšeným scanováním sítě z IP adres uvedených ve varování Národního úřadu pro kybernetickou a informační bezpečnost. Nemocnice v Olomouci byla na útok připravena zálohováním všech systémů. [11]

Kybernetické útoky na nemocnice ukázaly nejen slabou ochranu zdravotnických zařízení, ale především nedostatečnou organizovanost a ochranu IT infrastruktury moderních nemocnic. Mnoho daných zařízení využívá například operační systém Windows XP a má velké množství neošetřených zranitelností, které mohou útočníci využít ve svůj prospěch a získat úplný vzdálený přístup. Problémem bývají i ponechaná původní hesla pro daná zařízení. Výchozí hesla pachatelé snadno dohledají v manuálech na internetu.[12]

Kybernetický útok na OKD

Obdobným způsobem jako v případě nemocnice v Benešově byl proveden hlavní útok na těžební společnost OKD z Karvinska dne 22. prosince 2019. Útočníkům se podařilo učinit nefunkční kompletní síť a veškeré servery společnosti OKD. První pokus o útok byl proveden o dva dny dříve 20. prosince. Proces těžby byl pozastaven do 27. prosince 2019. Mluvčí společnosti OKD uvedl, že provoz těžby uhlí byl pozastaven z preventivních důvodů. Nicméně dodal, že bezpečnost horníků nebyla ohrožena, jelikož například čidla metanu nebyla útokem ochromena. Naštěstí se v případě těžební společnost OKD nejedná o technologickou společnost ani není její výroba strategicky řízena výpočetní technikou. Proto nebyl rozsah škod tak vysoký jako u nemocnice v Benešově. Těžební společnosti byla způsobena škoda v řádu milionů korun. [13],[14],[15]

Vyjádření Národního úřadu pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost den před Štědrým dnem roku 2019 prostřednictvím svých webových stránek varoval před hrozbou botnetu Emtotet ve spojitosti s malwarem TrickBot a ransomwarem Ryuk. Malware Emotet nejčastěji pronikne do počítače poškozeného na základě otevření infikované přílohy phisingového emailu a následného spuštění makra. Emotet umí přesvědčit svou oběť o pravdivosti emailu pro zajištění otevření nakažené přílohy emailu. I přes legitimní jméno adresáta by si měl příjemce zkontrolovat emailovou schránku odesílatele emailu, která se často liší. V danou chvíli by měl člověk zpozornět a nejlépe si pravost emailu ověřit u možného odesílatele například telefonickým zkontaktováním skutečné osoby odesílatele na základě ověřeného telefonického kontaktu z minulosti. Národní úřad pro kybernetickou a informační bezpečnost také upozornil, aby příjemci nepovolovali makra po otevření přílohy emailu. Jestliže příjemce nakonec infikovaný soubor stejně otevře, Emotet zajistí stažení Trickbotu do počítače oběti. TrickBot je schopen posbírat citlivá data oběti, jakými jsou třeba přihlašovací jména, hesla, registrové klíče, emaily, data z internetových prohlížečů. Získáním přihlašovacích údajů, prolomením slabých hesel či využití zranitelností EternalBlue u neaktuálních systémů je schopen se rozšířit v lokální síti. Pro znesnadnění svého odhalení Trickbot zajistí vypnutí služby Windows Defender. Až útočníci získají potřebné informace od své oběti, může dojít k instalaci ransomwaru Ryuk. Ryuk provede zašifrování dat oběti a pro jejich dešifrování vyžaduje uhrazení definované částky. Národní úřad pro kybernetickou a

informační bezpečnost nedoporučuje útočníkům zaplatit požadované výkupné, jelikož není zaručeno, že útočníci data skutečně dešifrují. Především apeloval na pravidelné offline zálohy dat, kterými by potenciální oběti v případě úspěšného útoku předešli výrazným škodám. Rovněž je institucím doporučováno mít aktuální antivirový program, logicky segmentovanou síť, pravidelně aplikovat bezpečnostní aktualizace, využívat silná hesla, omezit otevřené služby v síti, provádět kontroly stavu a konzistence záloh. Pro zaměstnance organizací je vhodné zajistit pravidelná školení v oblasti kybernetické bezpečnosti se zaměřením na aktuální kybernetické hrozby pro daný podnik. [16]

Koncem ledna 2020 Národní úřad pro kybernetickou a informační bezpečnost aktualizoval informace o hrozbě Emotet, Trickbot, Ryuk. Nově organizacím doporučil blokování archivní typy souborů s příponami LNK, které umožňují šíření viru. Upozornil na phisingové emaily v českém jazyce bez pravopisných chyb, které vyžadují zaplacení pohledávek, vyzvednutí zásilky a jiné. Přílohami daných emailů bývají soubory s koncovkami doc nebo docx. Dokumenty po jejich otevření požadují spuštění maker nebo povolení úprav pro popuštění chráněného režimu. V případě, že oběť provede otevření přílohy, dochází ke spuštění viru. Běžný uživatel nemusí být schopen rozeznat, že došlo k infikaci. Dále informoval o typickém chování Trickbotu, který kopíruje názvy skutečných souborů do škodlivých souborů s koncovkou jse. V případě objevení takových souborů v počítači by měl uživatel o dané skutečnosti informovat správce. Doporučil také nepoužívat administrátorský účet pro standardní práci na počítači. [17]

ZÁVĚR

Tento článek se zabýval kybernetickou bezpečností během šíření nemoci COVID-19. Byly zmíněny nové hrozby, se kterými se podniky musely vypořádat. V případě institucí byly uvedeny nemocnice, které podlehly kybernetickému útoku v daném období a také nemocnice s úspěšným odražením útoku.

Daný článek vznikl v rámci projektu IGA/FAI/2021/008 za podpory Interní grantové agentury Univerzity Tomáše Bati ve Zlíně.

SEZNAM POUŽITÉ LITERATURY

[1] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

[2] Současné trendy podvodníků - vishing a spoofing. *Policie.cz* [online]. Policejní prezidium ČR, 2021 [cit. 2021-07-30]. Dostupné z: https://www.policie.cz/clanek/web-informacni-servis-zpravodajstvi-soucasne-trendy-podvodniku-vishing-a-spoofing.aspx

[3] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0.

[4] Novinář zamával ministrům, vniknutím na uzavřené jednání překvapil sám sebe. *Idnes.cz* [online]. Idnes, 2020 [cit. 2021-07-30]. Dostupné z: https://www.idnes.cz/zpravy/zahranicni/nizozemsky-novinar-videokonference-ministri-obrany-eu.A201121_191249_zahranicni_misl

[5] Ukliknutí stálo nemocnici v Benešově 40 milionů. Kyberútok začal otevřením přílohy. *Lidovky.cz* [online]. Lidovky.cz, 2020 [cit. 2021-08-06]. Dostupné z: https://www.lidovky.cz/domov/ukliknuti-stalo-nemocnici-v-benesove-40-milionu-kyberutok-zacal-kliknutim-na-prilohu.A200115_201359_ln_domov_vlh

[6] Na nemocnici v Benešově útočil ruský virus Ryuk. Jermanová odmítá, že by někdo požadoval výkupné. *IRozhlas* [online]. IRozhlas, 2020 [cit. 2021-08-04]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nemocnice-benesov-kyberneticky-utok-ransomware-vykupne-ochrana-osobnich-udaju_2001140615_cha

[7] Kyberútok na nemocnici v Benešově způsobil škodu přes 59 milionů. Pachatele se vypátrat nepodařilo. *IRozhlas* [online]. IRozhlas, 2020 [cit. 2021-08-04]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/kyberutok-kyberneticky-utok-nemocnice-v-benesove-skoda-pachatel-hacker_2008180912_ako

[8] Zničení infrastruktury Emotet. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Národní úřad pro kybernetickou a informační bezpečnost, 2021 [cit. 2021-08-04]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1683-zniceni-infrastruktury-emotet/

[9] Brněnská nemocnice čelí kybernetickému útoku, neoperuje a převáží pacienty. *IDnes* [online]. IDnes, 2020 [cit. 2021-08-06]. Dostupné z: https://www.idnes.cz/brno/zpravy/brno-nemocnice-fakultni-nemocnice-kyberneticky-utok.A200313_071531_brno-zpravy_bur

[10] Kybernetický útok stál nemocnici v Brně desítky milionů, klesly odběry krve. *IDnes* [online]. IDnes, 2020 [cit. 2021-08-06]. Dostupné z: https://www.idnes.cz/brno/zpravy/fakultni-nemocnice-brno-kyberneticky-utok-skody-odber-krve.A200417_093436_brno-zpravy_krut

[11] Ostravská nemocnice odrazila kybernetický útok, vyřazení sítě v době epidemie zůstává velkou hrozbou. *IRozhlas* [online]. IRozhlas, 2020 [cit. 2021-08-06]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nemocnice-ostrava-kyberneticky-utok_2004171249_jak

[12] Hackerský útok na bohunickou nemocnici: Pachatelům může hrozit i dvanáct let. *Brněnskýdeník.cz* [online]. Brněnskýdeník.cz, 2020 [cit. 2021-08-06]. Dostupné z: https://brnensky.denik.cz/zpravy_region/brno-nemocnice-hacker-bohunice.html

[13] OKD přerušila těžbu ve všech dolech. Hackerský útok ochromil její počítačovou síť. *Lidovky.cz* [online]. Lidovky.cz, 2019 [cit. 2021-08-09]. Dostupné z: https://www.lidovky.cz/byznys/okd-okamzite-prerusila-tezbu-ve-vsech-dolech-hackersky-utok-ochromil-pocitacovou-sit-firmy.A191223_171939_firmy-trhy_vag

[14] Společnost OKD obnovuje těžbu po hackerském útoku. Experti pro ni vytvořili oddělenou počítačovou síť. *IRozhlas* [online]. IRozhlas, 2019 [cit. 2021-08-09]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/okd-doly-tezba-karvina-hackersky-utok-hornici-kyberbezpecnost-nukib-it-kyberutok_1912271142_gak

[15] OKD má po útoku hackerů opět plně funkční hlavní PC systémy. Škoda činí miliony. *Deník.cz* [online]. Deník.cz, 2020 [cit. 2021-08-09]. Dostupné z: https://www.denik.cz/regiony/okd-ma-po-utoku-hackeru-opet-plne-funkcni-hlavni-pc-systemy-skoda-cini-miliony-20200223.html

[16] Varování o hrozbě Emotet-Trickbot-Ryuk. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Národní úřad pro kybernetickou a informační bezpečnost, 2019 [cit. 2021-08-06]. Dostupné z:

https://www.nukib.cz/cs/infoservis/hrozby/1478-varovani-o-hrozbe-emotet-trickbot-ryuk/

[17] Aktualizace informací o hrozbě Emotet-Trickbot-Ryuk. Národní úřad pro kybernetickou a informační bezpečnost [online]. Národní úřad pro kybernetickou a informační bezpečnost, 2020 [cit. 2021-08-06]. Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/1483-aktualizace-informaci-o-hrozbe-emotet-trickbot-ryuk/