Redamp.io

WEBINÁŘ PRO ŽIVNOSTNÍKY A MALÉ FIRMY

Jedno kliknutí.
A celá firma stojí.

Ransomware zamkne vaše data a chce výkupné.
Jak se bránit a co dělat, když přijde.



ING. DOMINIK MALČÍK, PH.D. · REDAMP.IO · LISTOPAD 2026

Pojištěná firma s 500 kamiony.
Útok nejspíš začal uhodnutým heslem.

158 let

historie britského dopravce Knights of Old ze skupiny KNP.

Po útoku v roce 2023 skupina skončila v insolvenční správě. O práci přišlo asi 700 lidí.

ZDROJ: BBC PANORAMA, R. BILTON, 21. 7. 2025

Zamknou vám data.
Pak chtějí výkupné.

Chtějí peníze za odemčení a často i za nezveřejnění ukradených dat.
Zaplacení nic z toho nezaručuje.

PLÁN NA 30 MINUT

Dnes tři otázky.

01

Jak útok probíhá a kudy přijde?

02

Jak se bránit?

03

Co dělat, když se to stane?

Odnesete si tři věci, se kterými můžete začít ještě dnes večer.

Útok nezačíná zamčenými daty. Začíná otevřenými dveřmi.

Jak útok probíhá a kudy se útočník dostane do firmy?

Útok začíná potichu.
Výkupné přijde až nakonec.

01 Proniknutí

Útočník získá přístup do vašeho počítače, telefonu nebo sítě.

02 Průzkum a šíření

Může kopírovat vaše data a ničit zálohy. Příprava útoku může trvat dny.

03 Zašifrování

Škodlivý program během chvíle zamkne vaše soubory: dokumenty, účetnictví, fotografie.

04 Vydírání

Zpráva, kam a do kdy poslat výkupné, obvykle v kryptoměně. Často i s hrozbou zveřejnění dat.

Jak se útočníci dostanou dovnitř?
Například těmito cestami.

Podvodné zprávy a telefonáty

Podvržená faktura nebo výzva s nebezpečnou přílohou či odkazem, falešná „podpora“ po telefonu.

Neaktualizovaný software

Chyba v systému nebo programu, kterou jste neopravili, protože jste aktualizaci odložili.

Slabé nebo ukradené heslo

Útočník se přihlásí za vás, když chybí druhé ověření.

Infikovaný web nebo USB

Program stažený z neprověřeného webu nebo nalezený flash disk zapojený do počítače.

PODVODNÝ E-MAIL

Faktura, která není faktura. Ověřte ji jinou cestou.

Co se může stát, když spustíte škodlivou přílohu:

- Tiše se spustí škodlivý program.
- Útočník získá přístup do počítače.
- Později může zašifrovat data a chtít výkupné.

Nečekaná příloha? Nejdřív zavolejte odesílateli na číslo, které znáte.



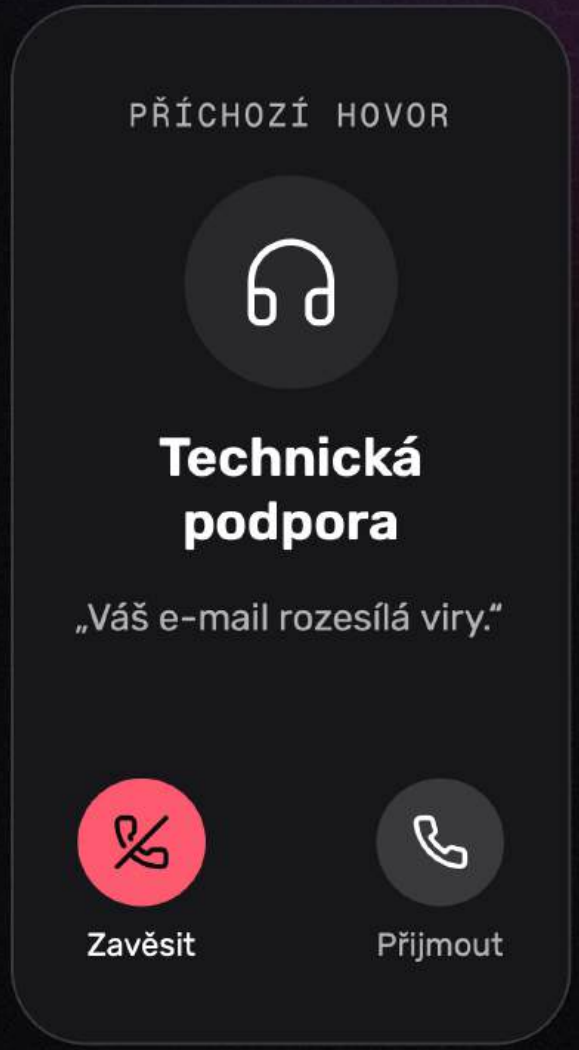
PODVODNÝ TELEFONÁT

Volá „IT podpora“.
Zavěste a volejte na známé číslo svého ajťáka.

Co se může stát, když volajícímu vyhovíte:

- Nainstalujete program pro „vzdálenou pomoc“.
- Útočník tím ovládá váš počítač.
- Později může zašifrovat data a chtít výkupné.

Na žádost volajícího nic neinstalujte a žádný kód nediktujte.



Bez dat nefakturujete.
Ani neprodáváte.

Účetnictví a fakturace

Může se zastavit fakturace a vyřizování objednávek.

Data klientů

Můžete ztratit přístup ke kontaktům, zakázkám i rozdělaným projektům.

Pokladna, sklad, výroba a e-shop

Dílna, prodejna nebo e-shop mohou přestat fungovat.

Osobní údaje a GDPR

Problémem je i jejich ztráta nebo nedostupnost. Nečekejte až na zveřejnění.

Útok zasáhl osobní údaje.
Rozhoduje riziko pro lidi.

VŽDY

Je to porušení

Únik i **nedostupnost** dat, třeba jen dočasná. Incident zdokumentujte zápisem.

RIZIKO PRO LIDI

Hlášení ÚOOÚ

Bez odkladu, pokud možno do 72 hodin od zjištění. Lze doplnit později.

VYSOKÉ RIZIKO

Informovat i lidi

Zákazníky nebo zaměstnance, kterých se data týkají.

Posouzení i hlášení může připravit odborník. Odpovědnost správce údajů nelze přenést na IT odborníka.

PLATFORMA · WINDOWS

Útok zašifruje vaše soubory.
A často i sdílené disky.

Zamkne dokumenty, účetnictví i síťové složky a nechá vzkaz s výkupným.



JAK SE BRÁNIT

- Automatické aktualizace Windows, neodkládat restart!
- Antivir zapnutý a aktuální.
- Běžná práce pod účtem bez práv správce.
- Vzdálený přístup jen přes své IT, nikdy na cizí výzvu.

PLATFORMA · MACOS

Mac není imunní. Ransomware je tu ale ne tak často.

JAK SE BRÁNIT

- Aplikace jen z App Store nebo od ověřených vývojářů.
- Varování o neověřené aplikaci neobcházejte.
- Vestavěnou ochranu nevypínejte (Gatekeeper, SIP, XProtect).
- Automatické bezpečnostní aktualizace zapnuté.
- Zálohujte přes Time Machine na odpojitelný disk.



PLATFORMA · ANDROID

Zamčený telefon. Falešná „policie“ chce pokutu.

Aplikace překryje obrazovku a zablokuje tlačítka. Výjimečně šifruje soubory.

JAK SE BRÁNIT

- Podporovaný a aktualizovaný telefon.
- Aplikace jen z Google Play, ne z odkazů.
- Může pomoci nouzový režim a odinstalace škodlivé aplikace. Když nepomůže, kontaktujte odborníka.
- Fotky a data mějte zálohované.



PLATFORMA · IPHONE A IPAD

Falešná výzva k zaplacení. Telefon přitom nemusí být napadený.

Aplikace jsou od sebe oddělené.

JAK SE BRÁNIT

- Falešnou výzvu v Safari zavřete, nic neplaťte.
- Účet Apple chraňte dvoufaktorovým ověřováním.
- Smazané fotky lze obvykle obnovit do 30 dnů.
- Neznámé profily ani správu zařízení nepovolujte.



Pět kroků.
S většinou můžete začít dnes večer.

Záloha, druhé ověření, aktualizace, opatrnost u e-mailu a antivir.

Zálohujte podle 3-2-1.
A obnovu vyzkoušejte.

Ověřená a nezasažená záloha vám pomůže obnovit provoz bez výkupného.

- Zálohujte podle toho, kolik práce si můžete dovolit ztratit.
- Alespoň jednu zálohu chraňte před smazáním i přepsáním.
- Synchronizace do cloudu sama nestačí.
- Obnovu zkoušejte alespoň jednou za pololetí.

Záložní disk po zálohování odpojte a uložte jinde.

3 **3 kopie dat**
Originál a dvě zálohy.

2 **2 různé typy úložišť**
Například externí disk a zálohovací cloud.

1 **1 kopie mimo provozovnu**
Ochrana i před požárem nebo krádeží.

KROK 2 Z 5 · DRUHÉ OVĚŘENÍ

Heslo nestačí.
Zapněte druhé ověření.

Samotné ukradené heslo pak útočníkovi zpravidla nestačí.

- Nejdřív e-mail, pak účetnictví a cloud.
- Kde to služba nabízí, použijte přístupový klíč (passkey).
- Obnovovací kódy uložte bezpečně, mimo telefon.
- Pro každý účet jiné dlouhé heslo ve správci hesel.

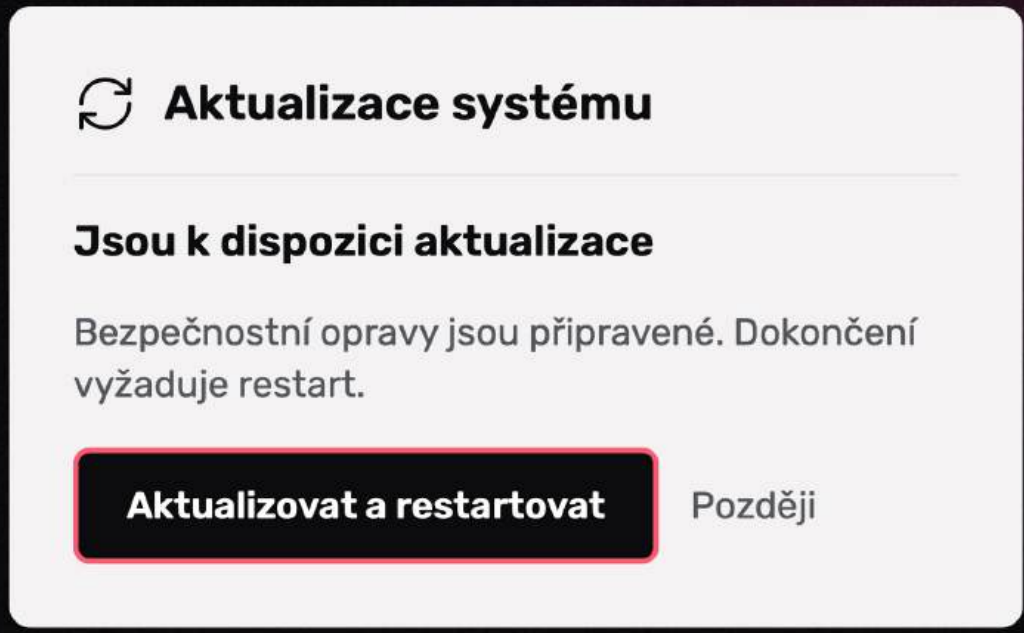
Kódy nikomu nesdělujte a přihlášení, které jste nezačali, neschvalujte.



Aktualizujte dnes.
Ne zítra.

Aktualizace opravují chyby, kterými se útočníci dostávají dovnitř.

- Zapněte automatické aktualizace systému i aplikací.
- Platí pro počítač, telefon, prohlížeč i router.
- Přejděte na podporovaný systém nebo zařízení.



Hlášku „Aktualizovat a restartovat“ neodkládejte.

Příloha nebo odkaz? Nejdřív ověřte.

Neotevírejte přílohy a neklikejte na odkazy, které nečekáte nebo které působí podezřele.

- Nečekaná faktura? Volejte na známé číslo.
- Spěch a výhrůžky jsou varovný signál.
- Podezřelou zprávu nahlaste IT, dál ji neposílejte.

Podpořte kolegy, aby podezření hlásili hned a bez obav.

Krátká kontrola před kliknutím

- ✓ Čekal jsem tuhle zprávu?
- ✓ Sedí adresa i obsah?
- ✓ Netlačí na mě spěchem?

Podvod může přijít i z napadeného účtu známého odesílatele.

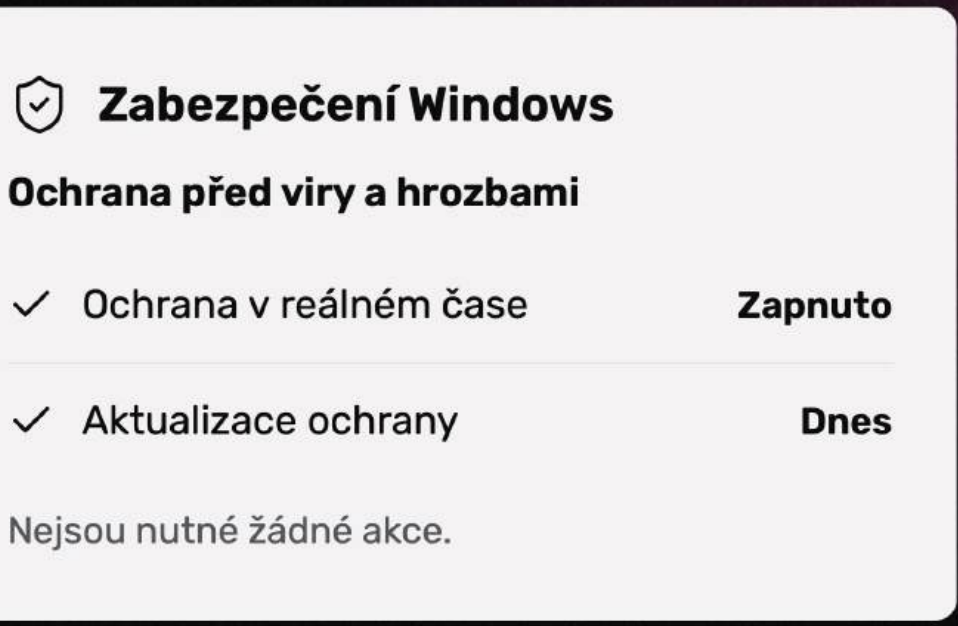
KROK 5 Z 5 · ANTIVIR

Antivir nevypínejte.
Varování berte vážně.

Zachytí mnoho škodlivých příloh a programů dřív, než se spustí.

- **Windows:** Microsoft Defender aktivní a aktuální.*
- **Mac:** Gatekeeper, SIP a XProtect nevypínejte.
- Programy instalujte jen z oficiálních zdrojů.
- Varování neignorujte a ochranu neobcházejte.

Antivir je jedna vrstva.
Bez záloh a aktualizací jen antivir nestačí.



* Místo Defenderu může být i jiný komerční antivir.

Útok se stal.
První kroky mohou omezit škody.

Co udělat v první hodině, komu zavolat a jestli platit výkupné.

Odpojit od sítě.
A zavolat odborníka.

1

Odpojit

Kabel ven a vypnout Wi-Fi. Omezíte šíření.

2

Vyfotit

Vyfoťte zprávu. Zapište čas zjištění.

3

Vypnout

Jen na pokyn odborníka nebo pokud zařízení nedokážete spolehlivě odpojit od všech sítí.

4

Nahlásit

Telefonem volejte IT a po poradě s IT odborníkem případně i policii: 158.

5

Obnovit

Do čistého prostředí, z ověřené zálohy, podle pokynů IT.

Záložní disk k napadenému počítači nepřipojujte. Mohli byste přijít i o tuto zálohu.

Nejste na to sami.
Tady je, komu zavolat.

KOMU	KDY A PROČ	KONTAKT
IT ODBORNÍK	Jako první, hned po odpojení. Poradí i s hlášením úřadům.	**číslo mějte i na papíře**
POLICIE ČR	Případně oznamte útok, nejlépe po poradě s IT odborníkem.*	**158**
POJIŠŤOVNA	Máte kyberpojištění? Volejte asistenční linku.	**z pojistné smlouvy**
BANKA	Hrozí-li zneužití plateb nebo účtu.	**z platební karty**

Zasažená osobní data klientů nebo zaměstnanců? Při riziku pro ně hlaste ÚOOÚ bezodkladně, pokud možno do 72 hodin od zjištění. Odpovědnost správce údajů nelze přenést na IT odborníka.

* Máte kyberpojištění? Jestli chce pojišťovna oznámení na policii, ověřte ve smlouvě nebo na asistenční lince.

Mám zaplatit výkupné?
Nedoporučujeme.

Žádná záruka

Nemáte jistotu, že klíč dostanete, ani že bude fungovat.

Opakovaný terč

Zaplacení vás neochrání před dalším vydíráním nebo útokem.

Financujete zločin

Výkupné platí další útoky na jiné malé firmy.

S odborníkem ověřte čistotu záloh a možnost obnovy.

Na nomoreransom.org zjistěte, zda pro váš případ existuje bezplatný dešifrovací nástroj.

Základní ochrana firmy.
A co dělat, kdyby se to stalo.

OCHRANA · S PRVNÍMI TŘEMI ZAČNĚTE DNES

- ✓ **Začít zálohovat podle 3-2-1**
- ✓ **Dvoufaktorové ověření na e-mailu**
- ✓ **Automatické aktualizace**
- ✓ Opatrnost u příloh a odkazů
- ✓ Antivir zapnutý a aktuální
- ✓ Jiné heslo pro každý účet

KDYŽ SE TO STANE

- ✓ Odpojit od všech sítí
- ✓ Vyfotit zprávu, zapsat čas zjištění
- ✓ Bez rady odborníka nevypínat*
- ✓ Zavolat IT a případně i policii 158
- ✓ GDPR: posoudit a případně hlásit, informovat
- ✓ Obnovit z ověřené zálohy, neplatit výkupné

* **Pokud si nejste jisti, že zařízení umíte spolehlivě odpojit od všech sítí, raději ho hned vypněte.**

Redamp.io

pro podnikavé

Děkuji.
Ptejte se.

Ing. Dominik Malčík, Ph.D.

Zakladatel a CEO, Redamp.io

dominik.malcik@redamp.io • +420 724 844 313

Více o Redamp.io

redamp.io →