Pravidelný bezpečnostní dýchánek

- Skákejte mi do řeči s dotazy a připomínkami.
- Zásadní: Pokud vám něco přijde nerealistické a víte, že to nebudete dělat, tak to prosím řekněte :) Něco s tím uděláme, je to mnohem lepší než mi něco odkývat a pak to tiše ignorovat.

1. Proč

Často se vůbec neřeší „proč“, bere se to jako evidentní. Chci stručně zopakovat pár důvodů, ať máte větší motivaci.

Proč to chceme řešit?

- Máme data uživatelů
- Máme pověst, o kterou nechceme přijít
- Naše pověst částečně stojí na digitálních kompetencích
- Říkáme, že víme, jak na to. Víme? :)

Proč to chceme řešit pravidelně?

- „Zabezpečená organizace“ je něco jako „posečený trávník“
- Proto se budeme k tématu vracet, nejspíš jednou za 1/4 roku

Proč to chceme řešit synchronně?

- Chceme si to vyzkoušet, časem může být část async.
- Je dobré to projít a sdílet společně, i u cizího příběhu vás může něco trknout

> c.d

2. Bezpečnostní minimum

- Tohle jsou pro naši organizaci absolutně nepodkročitelné věci.
- Nějaký bezpečnostní incident se nám může stát vždycky, ale pokud nebudeme dodržovat tyhle pravidla a něco se nám stane, budeme za idioty. Oprávněně.

> c.d

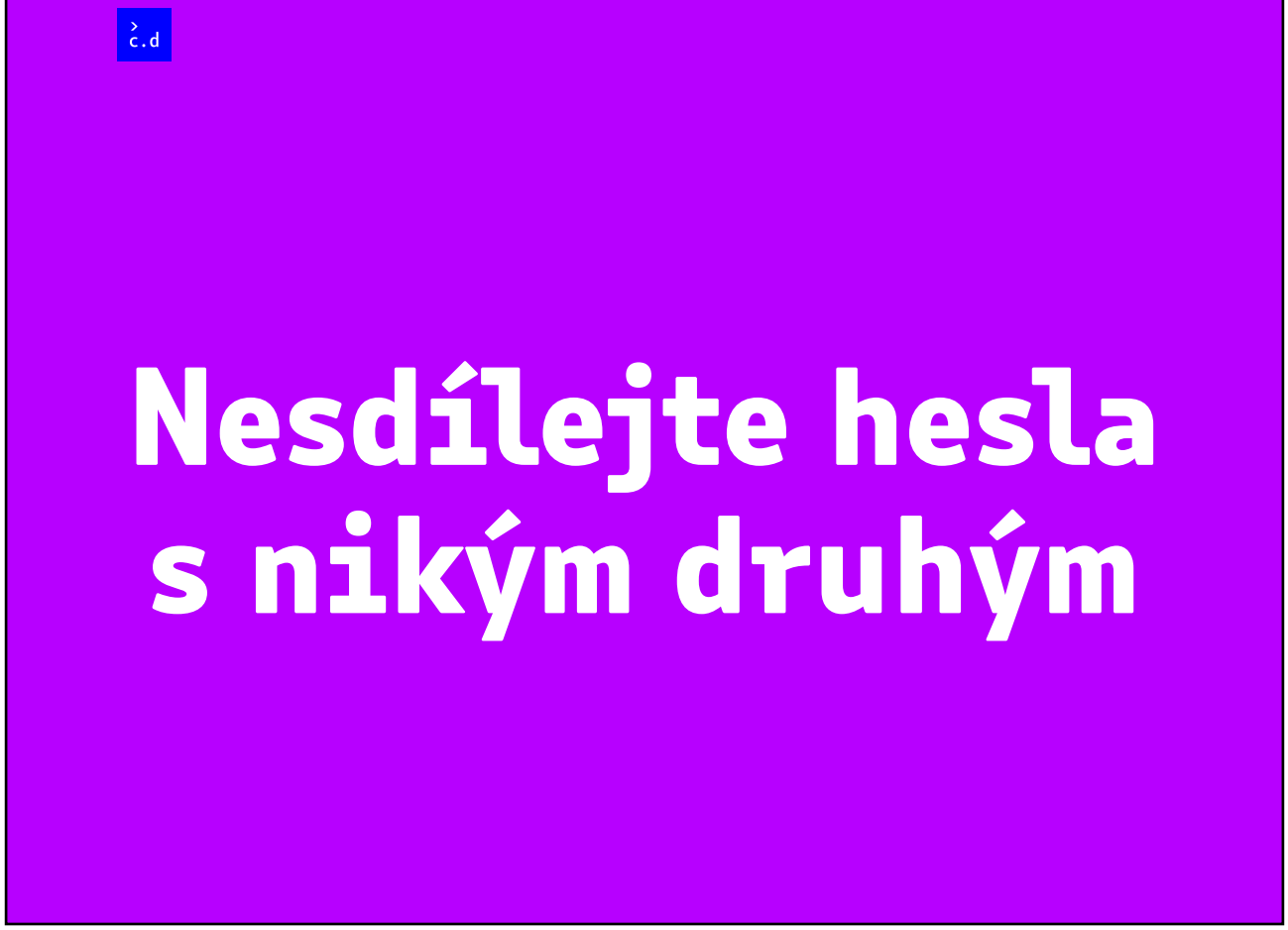
Hesla <3

Nepoužívejte hesla, která si dokážete zapamatovat

- Pokud si heslo dokážete zapamatovat, nejspíš je příliš slabé (pro zájemce: útoky hrubou silou)
- Existuje jediná výjimka, o které si řekneme později (správce hesel).
- I kdybyste si heslo dokázali zapamatovat, je tu další pravidlo:

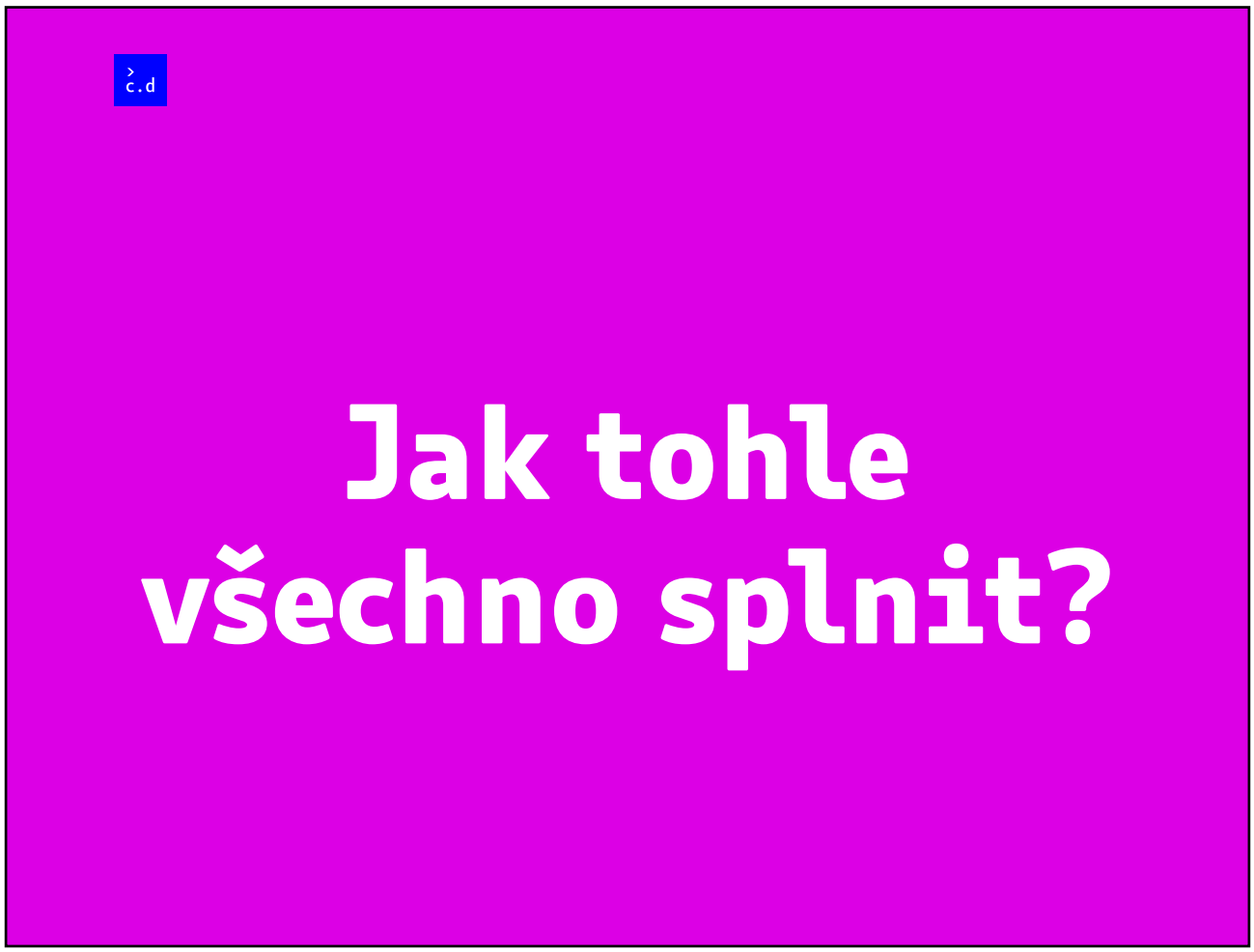
Nepoužívejte jedno heslo pro víc různých služeb

- Když jedné službě uteče databáze hesel (děje se pravidelně), často se vám pak útočník přes sdílené heslo dokáže dostat i do ostatních služeb.
- Co služba, to heslo.



- Proč byste to dělali?
- Jakým kanálem to heslo můžete předat? U většiny kanálů zůstane někde v historii, kde ho může někdo dohledat.
- Když už musíte, můžete poslat část jedním kanálem (Slack) a část jiným (SMS). Ale nedělejte to.
- Související pravidlo:

- Když používáte nějakou službu, měli byste mít samostatný účet pro každého z týmu.
- Když sdílíte účet, musíte nějak sdílet i hesla, a to je z principu problematické – viz předchozí bod.
- Nemůžete reálně použít MFA (podrobnosti později). Často se i bez MFA můžete dostat do potíží (přihlášení z atypického místa + kontrola telefonem).
- Zhoršuje se auditovatelnost – kdo ze všech těch uživatelů, co účet sdílí, něco udělal?



Tohle byla řada zákazů, pojďme se na to podívat z pozitivní stránky – co byste měli dělat.

- Hlavní heslo pro odemčení správce hesel je to jediné, které si můžete (a většinou i musíte) pamatovat.
- Většinou vám automaticky doplní heslo do přihlašovacího dialogu na webu.
- Pokud ne, možná nejste na tom správném webu…? :)
- Správce se často postará i o synchronizaci hesel napříč platformami (notebook, telefon, stolní počítač).
- Kdo co používáte?

Používejte autentizaci druhým faktorem

2FA – *second factor auth*
MFA – *multi factor auth*

- Faktory: něco si pamatuju (heslo), něco mám (klíč, HW token), něco jsem (biometrika).
- Kombinace víc faktorů výrazně zvyšuje bezpečnost.
- Jeden faktor je heslo, druhý faktor například SMS nebo kód z autentizační kalkulačky (něco mám – telefon).
- U důležitějších služeb používejte vždycky.
- Email je základ vaší digitální identity – MFA nutné.

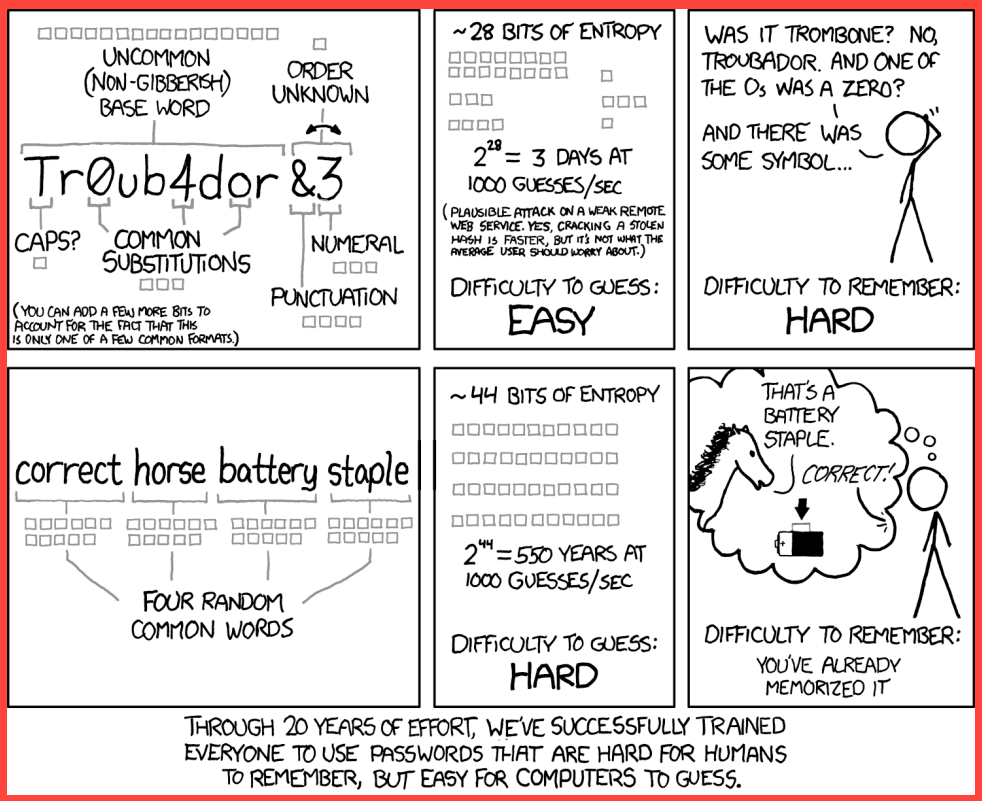
> c.d

Bezpečnostní tipy

Frázová hesla

- Furt si musíte pamatovat aspoň heslo k počítači a heslo ke správci hesel.
- Tahle hesla musí být dostatečně „komplikovaná“, jinak je všecko v pytli.
- Taky ale musí být zapamatovatelná, jinak je všecko v pytli.
- Jde to vůbec dohromady? Jde!

> c.d



Anketa: Jak jste na tom? Máte složité heslo, které si pamatujete, složité heslo, které si nepamatujete, jednoduché heslo, něco jiného?

Tipnete si nejčastější typ útoku?

Social Engineering & Phishing

- Kolega vám napíše, že potřebuje v rychlosti zaplatit novou službu, tady je QR kód / odkaz pro platbu.
- Často je to zdánlivě někdo, koho znáte. V dnešní době to klidně může být i hlasová zpráva nebo video.
- Dokonce to může být i v realistickém kontextu – viz scamy na Vintedu nebo doručovacích službách.
- Častý je důraz na spěch, protože spěch vám odebírá několik bodů IQ. Lidi v presu dělají chyby.
- Zvykněte si ptát se těch lidí na potvrzení buď bezpečnostní otázkou („co jsme měli včera k obědu?“) nebo druhým kanálem (SMS, sociální síť, …).
- Když potřebujete od někoho platbu nebo podobně, klidně jim rovnou tohle riziko sami připomeňte.
- Nemusí jít jen o peníze, ale i o data.

Hardwarová bezpečnost

- Zvykněte si zavírat / zamykat počítač, když od něj odcházíte ve sdíleném prostředí.
- Zapněte si šifrování dat na disku / v telefonu. Kdyby mi někdo ukradl notebook, pobrečím si nad hardwarem, ale vím, že k datům se nikdo nedostane.
- Pokud disk není šifrovaný, věnujte mu pozornost při případném prodeji nebo vyhazování hardwaru.

Pracovní × osobní prostředí

- Pokud kliknete na nějaký nezdravý odkaz, můžete kompromitovat všechny služby, ke kterým jste zrovna přihlášení.
- Kiksy v osobním brouzdání se vám tak můžou snadno přenést i na pracovní věci.
- Někdo má na osobní věci samostatný počítač.
- Realisticky jde ale mít aspoň samostatný profil v prohlížeči.
- Je to i velmi praktické, nemíchá se vám historie prohlížení a nemusíte donekonečna přepínat účty v Googlu, Trellu, …
- V úvahu docela snadno připadá i samostatný uživatelský účet.

Zvykněte si dělat věci správně

- Dělejte věci správně, i když to zrovna „není potřeba“, jinak je nebudete dělat správně, ani když to zrovna bude potřeba. (Vynášení koše.)