Lidský faktor trochu jinak

Úvod

- Uživatelé – fenomén, který představuje opravdu velké nebezpečí, a kterému se špatně brání.
- Větší nebezpečí ?

Kdo jsou odpovědní pracovníci ?

- Management a vedoucí pracovníci
- Pracovníci finančních a business oddělení
- Pracovníci IT oddělení
- Na koho jsme zapomněli ?
- Pracovníci security oddělení

Management a vedoucí pracovníci

- Neznalost reálných hrozeb a jejich možných důsledků
- Podceňování hrozeb, na které jsou upozorňováni
- Neochota naslouchat pracovníkům IT oddělení
- Podceňování významu vzdělávání a profesionálních služeb

Anketa mezi britským managementem

Anketní otázka: „Jaké jsou největší nebezpečí pro vaši organizaci v oblasti informační bezpečnosti?“

- 42% útočník změní naše webové stránky (kosočtvereček na hlavní stránce opravdu dobrou vizitku nedělá, ale zdaleka to není nejhorší možnost)
- 30% čtení firemních mailů útočníkem a jejich zveřejnění
- 24% zveřejnění našich důvěrných dat
- 4% ostatní

Závěr ankety je jasný: Management se nejvíce bojí ostudy, ale neuvědomuje si skutečná nebezpečí.

Co chybí ?

Pracovníci business oddělení

- Neznalost reálných hrozeb a jejich možných důsledků
- Podceňování hrozeb, na které jsou upozorňováni
- Neochota naslouchat pracovníkům IT oddělení
- Neopodstatněně vysoké sebevědomí
- Špatně nastavené priority

Pracovníci IT oddělení

- Neznalost reálných hrozeb a jejich možných důsledků
- Podceňování hrozeb, na které jsou upozorňováni
- Neochota se vzdělávat
- Neopodstatněně vysoké sebevědomí
- Špatně nastavené priority

Všichni

- Slepá důvěra „profesionálům“
- Neochota přiznat chybu včas (dokud lze relativně snadno napravit)
- Vystačíme si sami
- Bezpečnost je pro banky
- Špatně nastavené priority

Příklady

Sazka

Vývoj webové aplikace na zakázku

Vývoj a správa webu

Správa mailů a DNS

A mnoho dalších

Sazka

- Nepovedená marketingová akce
- Únik osobních údajů

Atlas.cz

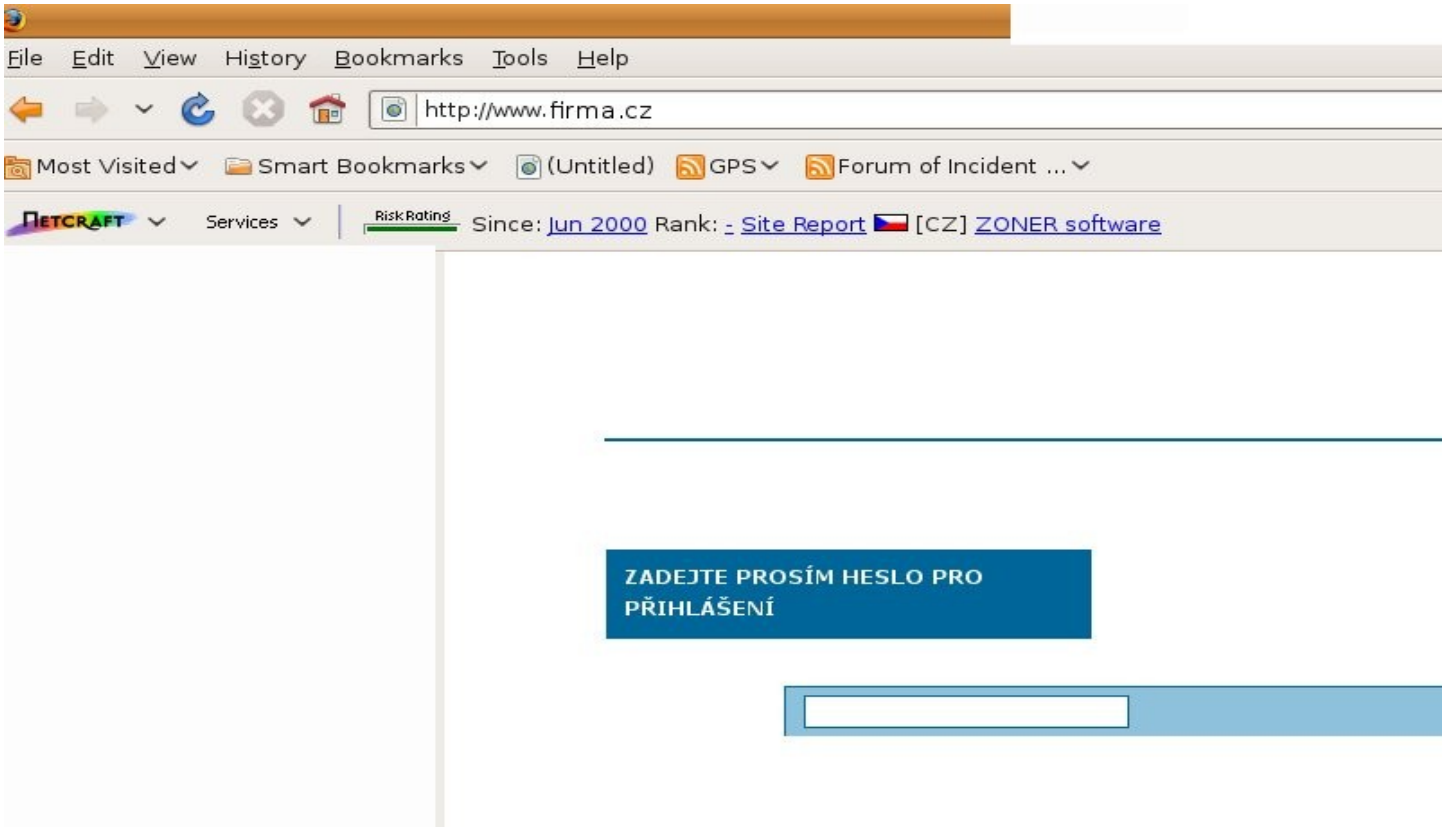
- Poslaní jména a hesla uživatele
- Listing uživatelů

Vývoj webové aplikace na zakázku

- Objednávka vývoje aplikace
- Zcela neodpovídající počáteční analýza
- Zpočátku téměř nulová kontrola
- Bagatelizace nalezených problémů
- Pohár trpělivosti přetekl.....soud

Vývoj a správa webu

- I takto může vypadat správa webu v podání „profesionálů“



Správa mailů a DNS

- I takto může vypadat správa webu v podání „profesionálů“

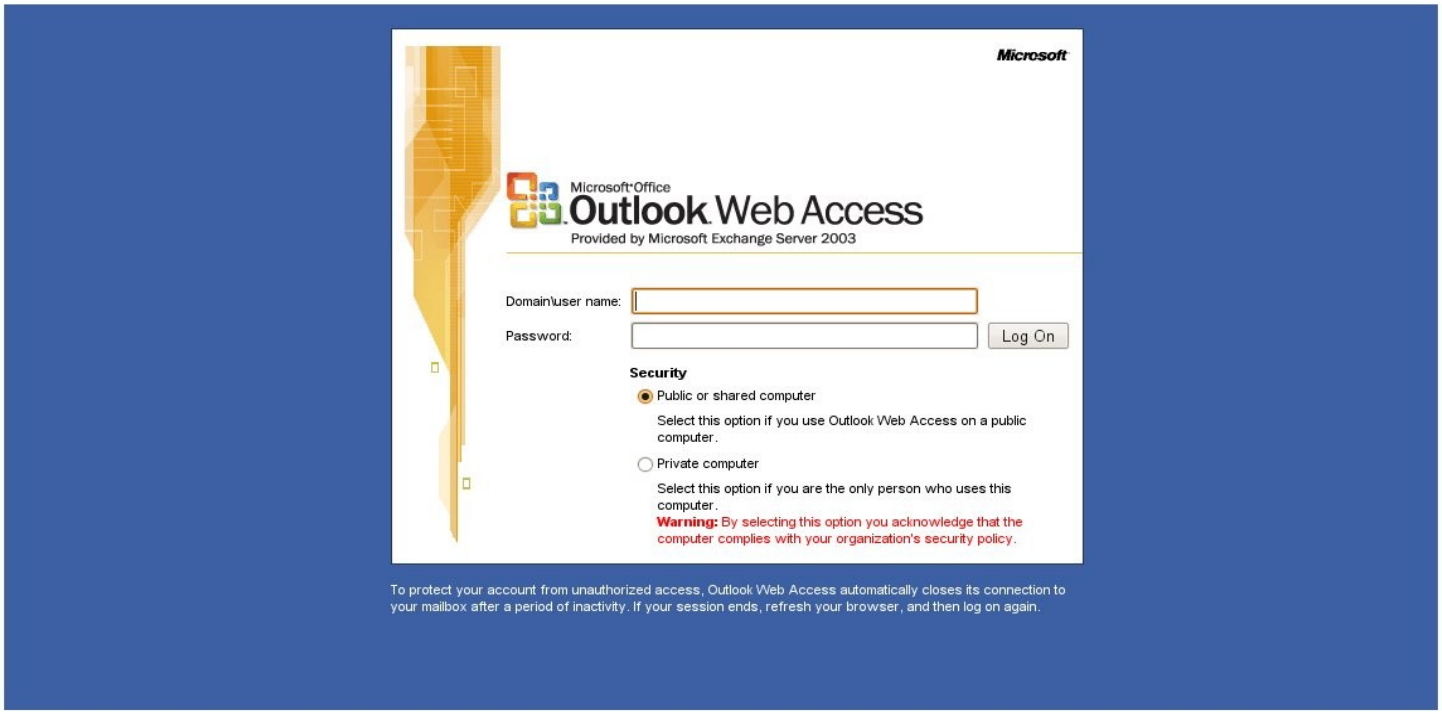
Firma, která toto spravuje, spravuje maily a DNS pro stovky domén

```
lui@aja:~$ su -
root@aja:~# nmap mail.vojdz.cz

Starting Nmap 4.03 ( http://www.insecure.org/nmap/ ) at 2009-02-17 19:24 CET
Interesting ports on fblc01.fbl.cz (82.100.63.86):
(The 1663 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE
21/tcp   open     ftp
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
143/tcp  open     imap
322/tcp  open     unknown
993/tcp  open     imaps
995/tcp  open     pop3s
3306/tcp filtered mysql
5432/tcp open     postgres

Nmap finished: 1 IP address (1 host up) scanned in 2.782 seconds
root@aja:~#
```

Správa mailů

- I takto může vypadat správa webu v podání „profesionálů“

Firma, která toto spravuje, spravuje maily a DNS pro stovky domén



Nové možnosti

- Penetrační testy
- Bezpečnostní audity webových aplikací
- Šifrovaná telefonie

- Omezená verze **zdarma**

Jedno až dvoudenní penetrační testy
Zjednodušený audit webové aplikace
Zápůjčka telefonů, které mezi sebou telefonují šifrovaně

Závěr

- Služby profesionálů - ANO
- Nepodceňovat rizika
- Vzdělávání je nedílnou součástí každé profese
- Interní IT není jen pro zlost
- Nikdo neumí vše
- Procesní bezpečnost (bezp. pol, hav.plány)
- Nastavení priorit
- I specilaizované firmy je třeba občas kontrolovat
- Sledování nových možností

Děkuji za pozornost


4Safety
Lidský faktor trochu jinak

Technických presentací mají hodně ostatní přednášející

Nebudu mluvit o žádných produktech, ale budu se snažit ukázat jinou stránku bezpečnostní problematiky.

Uživatelé – neznalost a nezodpovědné chování uživatelů je známá věc. To nic nemění na tom, že je nutné to stále připomínat, neboť metody, jak toho útočníci zneužívají se stále vyvíjí a je nutné na to reagovat. Toto je však předmětem jiné přednášky

Domnívám se, že existuje ještě daleko horší nešvar, který představuje o hodně vyšší nebezpečí. Jená se o zcela nevhodné chování odpovědných pracovníků.

Management – to je asi všem jasné a není třeba to dále rozvádět. Všichni asi tuší, že v této souvislosti máme na mysli spíše střední a vyšší management a nikoli managera prodejny u obchodného řetězce.

Pracovníci business oddělení – pod tímto na první pohled tajemným názvem se rozumíme pracovníky zodpovědné za nějaký větší projekt a to od jeho zadání až do úspěšného zakončení. Z poslední doby můžeme vzít jako přáklad internetové sázení, které se velmi rozmáhá díky změně v legislativě. Tomu se přizpůsobují i sázkové kanceláře a vyvíjejí (ať už vlastními silami nebo si nechávají vyvíjet) webové aplikace pro internetové sázení.

Pracovníci IT oddělení – zde se jedná zpravidla o interní administrátory

Pracovníci security departementu – security department nespadá pod IT a zodpovídá se managementu. Vedoucí sec. Departementu bývá zpravidla členem managementu. Tuto skupinu vynecháváme úmyslně, neboť v organizacích, kde toto oddělení existuje, má správné zařazení v hierarchii organizace a má skutečné pravomoce většina (nikoli všechny) zmiňovaných problémů neexistuje.

V této části budu mluvit o těch nejkřiklavějších skutečnostech.

Samozřejmě, že jsou i velmi osvícení pracovníci managementu, ale zatím se jedná bohužel spíše o vyjímky.

Management velmi často nezná možná nebetpečí. Samozřejmě to není myšleno technicky. Na to je v organizaci jiné oddělení.

Management skutečně nezná reálá rizika nejvíce ohrožující jejich společnost viz další slide.

Management má sklony bagatelizovat hrozby, na které je upozorňuje jejich vlastní IT oddělení či někdo „zvenku“ Typické jsou odpovědi

To se nás netýká

Koho by zajímala naše data

Ať si naše maily klidně přečtou. Nic tajného nemáme.

Tohle nemusíme řešit, to naši uživatelé nezvládnou.

Nejsme banka (tím se zpravidla myslí, že jediné instituce, které musí dbát o bezpečnost jsou banky.

Pokud na nebezpečí upozorňuje vlastní IT často se setkává s odpovědí Zase chcete koupit další hračku.

Pokud už se management rozhodne řešit bezpečnostní problematiku, má sklony koupit „samospasitelnou krabičku“. Mnoho firem bohužel slibuje, že nasazením jejich firewallu IPS apod. Práce končí. Udávají čísla že na první nastavení je třeba xx mina a následně xx min měsíčně. To je samozřejmě možné, ale bezpečnost organizace, která se těmito čísly řídí podle toho vypadá. Šení potřebuje stálý dohled a údržbu (aplikace nových firmware, udržování aktuálních pravidel, dokumentace, sledování událostí, reakce na ně atd.)

Je více než jasné, že „samospasitelná krabička“ neexistuje a bez dostatečně proškolených pracovníků nebo spolupráce s profesionální společností, která se nám o zmíněné řešení stará se jedná o vyhozené peníze.

Management často považuje peníze investované do vzdělávání vlastních pracovníků nebo do profesionálních služeb za vyhpzené peníze.

Ve GB byla provedena anketa. Agentura provádějící tuto anketu se ptala pracovníků managementu jaká je největší hrozba pro jejich společnost v souvislosti s informační bezpečností. Odpovědi jsou alarmující:

42% útočník změní naše webové stránky (kosočtvereček na hlavní stránce opravdu dobrou vizitku nedělá, ale zdaleka to není nejhorší možnost)

30% čtení fremních mailů útočníkem a jejich zveřejnění
24% zveřejnění našich důvěrných dat

4% ostatní

Závěr ankety je jasný: Management se nejvíce bojí ostudy, ale neuvědomuje si skutečná nebezpečí.

Vůbec nebyly zmíněny největší hrozby:

Získání důvěrných dat na zakázku konkurence.

Narušení integrity důvěrných dat (příklad s velkou státní zakázkou a modifikacá nákupního ceníku)

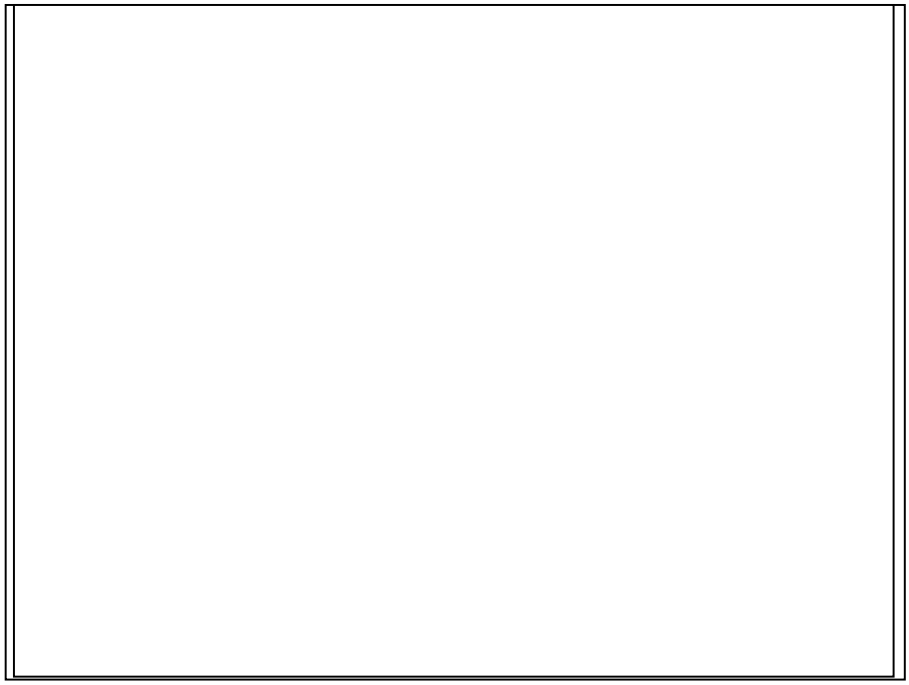
V této části budu mluvit o těch nejkřiklavějších skutečnostech.

Samozřejmě, že i v této skupině existují osvícení pracovníci, ale bohužel je jich minimum.

V drtivé většine případů tito lidé neznají skutečné hrozby. Pokud jsou na ně upozorňováni, mají tendenci tato upozornění bagatelizovat a podceňovat a ta, co na tato nebezpečí upozorňují označovat za paranoidní.

Častose chovají nepřiměřeně sebevědomě, kdy jejich sebevědomí pochází většinou z důležitosti a velikosti projektu, který řídí. Bohužel si neuvědomují, že svým chováním mohou svou společnost velmi významně poškodit.

V projektech, za které jsou zodpovědni mají zpravidla špatně nastavené priority a řídí se heslem „Nejdříve to musí fungovat a když zbyde čas a peníze, tak budeme řešit nějakou bezpečnost“ Každí, ldo s tím má zkušenosti ví, že bezpečnost je nutné řešit systematicky a to již ve fázi nývrhu projektu. Pokud se k tomu přistoupí dle zmíněného hesla, většinou na žádné řešení bezpečnosti nedojde. Když vyjímečně ano, je to o mnoho časově náročnější, dražší a logicky i nesrovnatelně nižší kvality.



V této části budu mluvit o těch nejkřiklavějších skutečnostech.

Na rozdíl od předchozích skupin, zde nejsou osvícení pracovníci vyjímkou, ale poměr je cca půl na půl.

Nicméně bohužel existuje cca 50% pracovníků IT oddělení (síťových administrátorů), kteří se domnívají, že instalace metodou „Next, Next, Finish“ je to nejlepčí, co prosvou organizaco mohou udělat. Zároveň se většinou mylně domnívají, že vše ví a jakékoli další vzdělávání nepotřebují. Tato část administrátorů má stejně špatně nastavené priority jako předchozí skupina.

Na případné upozornění o nevhodnosti používaného řešení z pohledu bezpečnosti reagují hláškou tybu „Bezpečnost se tadynikdy neřešila“, To je drobnost a děláte z toho vědu“ apod.

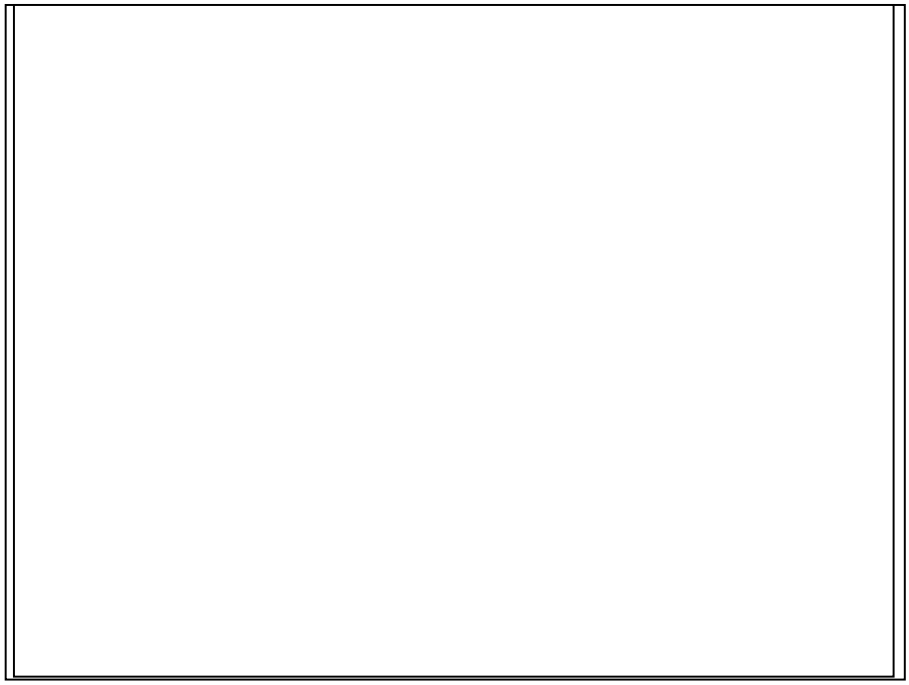
Některé problémy jsou napříč všemi zmoňovanými skupinami.

Pokud menší společnost dodává nějakou službu, či vývoj aplikace na zakázku za „rozumné“ peníze hledá se na ní každá chyba. Pokud tu samou službu dodává společnost,která se tváří dostatečně sebevědomě a účtuje si dostatečně vysokou cenu (vyšší jednotky až desítky milionů) projdou téměř jakékoli chyby či nedostatky.

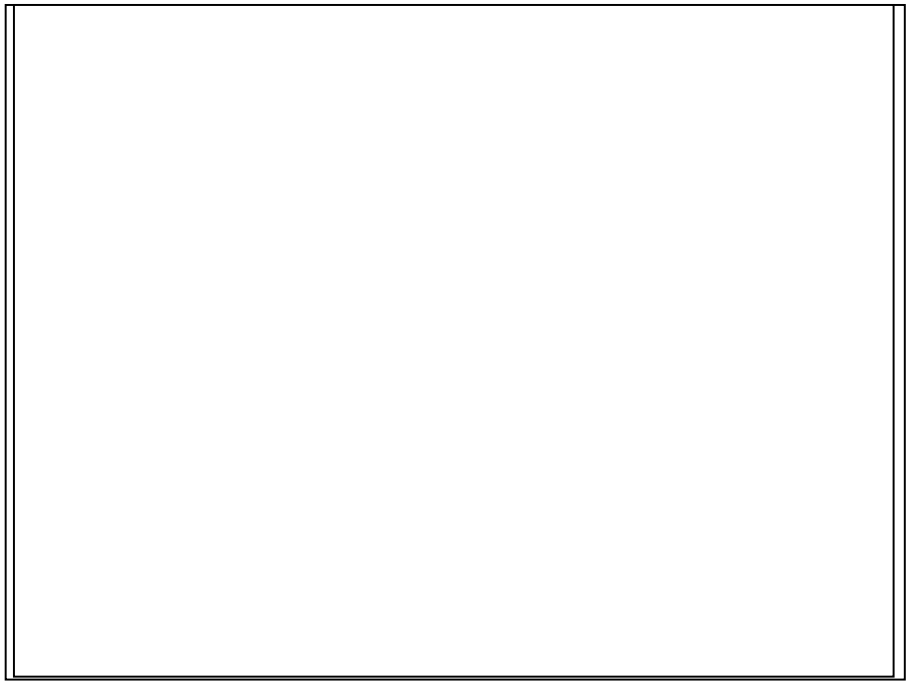
Existuje pochopitelně více důvodů, ale nejčastější jsou:

1) Když to stojí tolik peněz, tak jsou to skuteční profesionálové a vědí co dělají. Když říkají, že to musí byt takto, tak vědí proč a my to nemůžeme zkoumat. (Není důvod o zkoumat)

2) Když se vynaložilo tolik prostředků (peněz i času), ak se velmi obtížně vysvětluje nadřízeným (managementu, majielům), že se jednalo o „vyhozené“ peníze a je třeba začít s celým projektem od začátku.



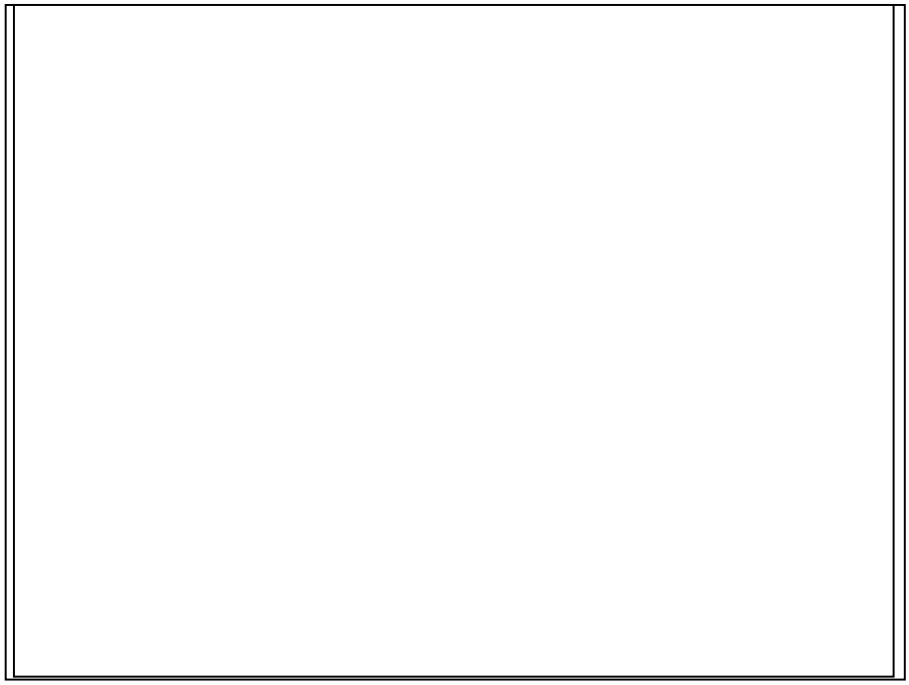
Společnost Sazka, a.s. spustila internetové sázení. Rozjezd projektu doprovázela marketingová akce, kdy každému novímu hráči dali 10.000 a později již jen 2.000 bodů na jeho účet, kdy tyto body mělo být možné na jedné sázce uplatnit max XY bodů a ještě k nim přidat nějaké vlastní peníze. Aplikace včask nneuměla kombinovat body a peníze a bylo možné utratit v podstatě neomezený počet bodů. Stačilo tedy najít sázku s nejnižším kursem a vsadit zmíněné 2000 bodů atím je proměnit na peníze. V tu chvíli Sazka dala, každému hráči 2.000 Kč



Společnost Sazka, a.s. spustila internetové sázení. Rozjezd projektu doprovázela marketingová akce, kdy každému novímu hráči dali 10.000 a později již jen 2.000 bodů na jeho účet, kdy tyto body mělo být možné na jedné sázce uplatnit max XY bodů a ještě k nim přidat nějaké vlastní peníze. Aplikace včask neuměla kombinovat body a peníze a bylo možné utratit v podstatě neomezený počet bodů. Stačilo tedy najít sázku s nejnižším kursem a vsadit zmíněné 2000 bodů atím je proměnit na peníze. V tu chvíli Sazka dala, každému hráči 2.000 Kč.

Sazka několikrát měnila herní řád a množí se spekulace, zda je to v souladu s naší legislativou, neboť sázková kancelář má povinnost tuto zmenu nahlásit tři dny předem na MF a Sazka tak údajně neučinila.

Později se zjistilo, že ve webové aplikaci, kterou Sazka pro internetové sázení je závažná bezpečnostní chyba a bylo snadno možné získat osobní údaje hráčů. Krátce po zveřejnění společnost Ecommerce, a.s. (která aplikaci nejen vyvinula, ale i servery s touto aplikací pro společnost Sazka, a.s. Provozuje) začla pracovat na odstranění zmíněné chyby. Ochotu organizací postavit se k obdobným problémům čelrm vidíme i na tom, že nekterá prohlašení pracovníků Sazky, byla přinejmenším hodně mlhavá. Přesto, že je obecněznámo, že na Slovensku je používána stejná aplikace společnost Sazka tvrdila, že hráčů na Slovensku se tento problém netýká.



Společnost Sazka, a.s. spustila internetové sázení. Rozjezd projektu doprovázela marketingová akce, kdy každému novímu hráči dali 10.000 a později již jen 2.000 bodů na jeho účet, kdy tyto body mělo být možné na jedné sázce uplatnit max XY bodů a ještě k nim přidat nějaké vlastní peníze. Aplikace včask neuměla kombinovat body a peníze a bylo možné utratit v podstatě neomezený počet bodů. Stačilo tedy najít sázku s nejnižším kursem a vsadit zmíněné 2000 bodů atím je proměnit na peníze. V tu chvíli Sazka dala, každému hráči 2.000 Kč.

Sazka několikrát měnila herní řád a množí se spekulace, zda je to v souladu s naší legislativou, neboť sázková kancelář má povinnost tuto zmenu nahlásit tři dny předem na MF a Sazka tak údajně neučinila.

Později se zjistilo, že ve webové aplikaci, kterou Sazka pro internetové sázení je závažná bezpečnostní chyba a bylo snadno možné získat osobní údaje hráčů. Krátce po zveřejnění společnost Ecommerce, a.s. (která aplikaci nejen vyvinula, ale i servery s touto aplikací pro společnost Sazka, a.s. Provozuje) začla pracovat na odstranění zmíněné chyby. Ochotu organizací postavit se k obdobným problémům čelrm vidíme i na tom, že nekterá prohlašení pracovníků Sazky, byla přinejmenším hodně mlhavá. Přesto, že je obecněznámo, že na Slovensku je používána stejná aplikace společnost Sazka tvrdila, že hráčů na Slovensku se tento problém netýká.

Nejmenovaná sázková kancelář si objednala vývoj aplikace pro sázení na svých pobočkách.

Vývoj si objednali u společnosti s velmi dobrými referencemi, jejíž pracovníci se dušovali, že s aplikacemi tohoto typu mají bohaté zkušenosti.

Vypracovali analýzu potřeb, postupů a cílů, která naprosto neodpovídala skutečným potřebám zákazníka. Na tuto analýzu se odvolává i smlouva.

Cca 7 měsíců se vše jen podepisovalo a platily se průbežné platby dle smlouvy. Po 7 měs. Jeden pracovník (který tím vůbec nebyl pověřený) aplikaci prohlédl a našel tam zcela zásadní problémy (jak funkční, tak bezpečnostní).

Následovala bagatelizace těchto problémů. Označování danného pracovníka jako neodborného, který se přece nemůže rovnat s profesionály dodavatele.

Jen pro ilustraci jeden z problémů byl, že aplikace využívá http (nikoli https) protokol. Dokonce i v té analýze pochybné kvality, na kterou se odvolává smlouva bylo jasně napsáno, že bude použit https protokol. Pracovníci dodavatele přesto tvrdili, že je to zbytečné a obavy z napadení jsou výmyslem paranoika, neboť napadení by bylo příliš složité. Všichni jak tu sedíme víme, že stačí obyčejný wireshark :)

Po dalších cca 5 měsících vývoje a odkladů došla zadavateli trpělivost a v tuto chvíli je celá věc u renomované právní kanceláře s tím, že chtějí odstoupit od smlouvy.

https://mail.rrc.cz/exchweb/bin/auth/owalogon.asp?url=http://www.4safety.cz/&reason=0

Správa mailů

- I takto může vypadat správa webu v podání „profesionálů“

Firma, která toto spravuje, spravuje maily a DNS pro stovky domén