Datacentrum Bosting

Štěpán Kobza

Brno 2022

Obsah

1 Úvod

Datacentrum Bosting se nachází v novostavbě dvoupodlažního domu v průmyslové zóně. Firma Bosting provozuje web hosting a hosting libovolných serverů. Aktuálně provozuje cca 1 000 webů a 100 specializovaných serverů, vše poskytuje pomocí virtualizace.

Firma Bosting je to malá, má 10 zaměstnanců, kteří jsou pravidelně školeni, dále mají zmapované všechny interní procesy v rámci bezpečnostní politiky firmy. Bosting se stal párkrát terčem kybernetických útoků, avšak všechny útoky proběhly bez větších potíží a nedošlo k žádné finanční ztrátě či odcizení dat.

2 Analýza

2.1 Identifikovaná aktiva

Tab. 1. Identifikovaná aktiva

Typ aktiv	Identifikovaná aktiva	Hodnota aktiv
Informace	Databáze webů	4
HW	Servery	5
	Notebook	3
	AP pro Wifi	2
	Switche	3
	Routery	3
	Diskové pole	5
	Vybavení serverovny	5
Software	SW pro virtualizaci	5
	Web hosting	5
	OS	3
	Databázové systémy	4
	Informační systém	5
Služby	Připojení k internetu	4

2.2 Hrozby a zranitelnosti

Tab. 2. Hrozby a zranitelnosti

Identifikovaná hrozba	Pravděpodobnost hrozby	Příklad zranitelnosti
Selhání hardware	5	náchylnost na přehřátí, prach a vlhkost u serveru
Selhání software	4	nepoužívání licencovaných programů, špatně napsaný kód
Kybernetický útok	5	DDos útoky, ransomware, špatný antivirus
Neúmyslná modifikace	2	špatné rozdělení práv uživatelů
Ztráta aktiv	3	špatně zabezpečená budova, ztracení dat
Výpadek elektřiny	4	přetížení elektrické sítě
Požár	1	zkrat el. obvodů, lidská chyba
Výpadek internetu	2	chyba na straně poskytovatele

2.3 Matice zranitelnosti

Tab. 3. Matice zranitelnosti

Matice zranitelnosti	**Popis aktiva**	Databáze webů	Servery	Notebook	AP pro Wifi	Switche	Routery	Diskové pole
Popis hrozby	**Hodnota aktiva**	4	5	3	2	3	3	5
	Pravděpodobnost hrozby							
Selhání hardware	5		4	3	2	2	2	3
Selhání software	4							
Kybernetický útok	5	4	5	3				
Neúmyslná modifikace	2	2						
Ztráta aktiv	3	3						3
Výpadek elektřiny	4			3	2	2	2	
Požár	1		3	2	1	1	1	3
Výpadek internetu	2							

Matice zranitelnosti	**Popis aktiva**	Vybavení serverovny	Web hosting	OS	SW pro virtualizaci	Databázové systémy	Informační systém	Připojení k internetu
Popis hrozby	**Hodnota aktiva**	5	5	3	5	4	5	4
	Pravděpodobnost hrozby							
Selhání hardware	5	2						
Selhání software	4		4	2	3	3	4	
Kybernetický útok	5					4	4	
Neúmyslná modifikace	2				3	2	2	
Ztráta aktiv	3						3	
Výpadek elektřiny	4	5						
Požár	1	3						
Výpadek internetu	2							4

2.4 Matice rizik

Tab. 4. Matice rizik

Matice rizik	**Popis aktiva**	Databáze webů	Servery	Notebook	AP pro Wifi	Switche	Routery	Diskové pole
Popis hrozby	**Hodnota aktiva**	4	5	3	2	3	3	5
	Pravděpodobnost hrozby							
Selhání hardware	5		100	45	20	30	30	75
Selhání software	4							
Kybernetický útok	5	80	125	45				
Neúmyslná modifikace	2	16						
Ztráta aktiv	3	36						45
Výpadek elektřiny	4			36	16	24	24	
Požár	1		15	6	2	3	3	15
Výpadek internetu	2							

Matice rizik	**Popis aktiva**	Vybavení serverovny	Web hosting	OS	SW pro virtualizaci	Databázové systémy	Informační systém	Připojení k internetu
Popis hrozby	**Hodnota aktiva**	5	5	3	5	4	5	4
	Pravděpodobnost hrozby							
Selhání hardware	5	50						
Selhání software	4		80	24	60	48	80	
Kybernetický útok	5					80	100	
Neúmyslná modifikace	2				30	16	20	
Ztráta aktiv	3						45	
Výpadek elektřiny	4	100						
Požár	1	15						
Výpadek internetu	2							32

3 Opatření

3.1 Selhání hardware

Proti selhání hardwaru můžeme předejít správným zacházením techniky. Ve firmě Bosting jsou nejnáchylnější na selhání servery, které se můžou například způsobením špatného chlazení přehřívat a vlivem toho se mohou zničit některé části serveru. Tudíž bych doporučil kvalitní chlazení serverovny, dále její pravidelné uklizení, aby se zamezilo většímu množství prachu. Servery bych zapojil do clusteru, abych v případě selhání jednoho serveru mohl dále poskytovat služby a nezpůsobil bych ztrátu danému odběratelovi mého hostingu.

3.2 Selhání software

Především používáním licencovaného softwaru se dá předejít jeho selhání. Důležitá je však jeho pravidelná aktualizace na zařízeních. V případě vlastního softwaru je důležité, aby daný kód byl řádně otestovaný a nebyla v něm chyba, která by způsobila selhání celého softwaru. Řada softwaru je zdarma, některé licencované softwary se jednou koupí a už se nemusí platit.

3.3 Kybernetický útok

Kybernetické útoky byly, jsou a budou. Důležité je umět jim předcházet. Takovým základním kamenem je dobře proškolený personál a kvalitní firewall, už tímhle se dá zamezit spousta problémům. Zaměstnanci by měli být poučeni o hrozbách v podobě phishingu a škodlivého malwaru. Důležité je také sledovat nepřetržitě provoz serverů. Musí se dobře vyhodnotit, co je normální provoz a co je vysoký provoz. V případě nějakého bezdůvodného vyššího provozu se připravit na případný DDoS útok a učinit potřebné obrané kroky. Například omezení přístupů, zavolání na provozovatele internetu, že jsme terčem DDoS útoky, zkusit přesměrovat provoz na masivnější servery, v posledním případě přežít daný útok. Důležité je pak celý daný incident nahlásit na Národní úřad pro kybernetickou a informační bezpečnost, který se daným incidentem bude zabývat. Určitě bych se nebál jako první věc investovat do dobrého firewallu, který dokáže spoustu věcí zachytit a dokážeme díky němu předejít i finančním ztrátám z důvodu nefunkčnosti serverů, pak bych doporučil antivirový programy, které můžou být i na free verzi.

3.4 Neúmyslná modifikace

Proti neúmyslné modifikaci musí být dobře nastavená bezpečnostní politika. Dále je to nastavení práv pro různé zaměstnance, účetní nepotřebuje přístup do systémového nastavení, obchodní zástupce nemusí mít přístup do konfigurace serverů, kde by mohl nastavit nějaké parametry, které by mohly vést až k nefunkčnosti daného serveru. Na koncových zařízeních (notebook, počítač) bych podmínil instalaci programů jenom pod přihlášením administrátorského účtu, který má jediný oprávnění programy instalovat.

3.5 Ztráta aktiv

Ztráta aktiv může být ve dvou variantách. První varianta je ztráta aktiv v podobě fyzického odcizení aktiv. Kvalitní zabezpečení budovy, jako jsou kamery, přístupové karty, kvalitní dveře a okna nejsou zbytečné. Vstupní investice je vyšší, ale dokáže výrazně snížit riziko jejich krádeže. Krádež dat je problém špatného zabezpečení sítě a souvisí především s kybernetickým útokem.

Druhá varianta je ztráta dat, které nejsou zálohované. Záloha dat je velmi důležitá a kladl bych na ni velký důraz. Záloha serverů by měla probíhat neustále, především dat a konfiguračních souborů na dvě diskové pole (jeden pro data, druhý pro konfigurační soubory) a pravidelně v noci provádět zálohu na disky, které se nachází mimo budovu, například v jiném datovém centru. Určitě dobré zálohování udělat co nejdříve, případně si zaplatit firmu, která nám se zálohováním pomůže.

3.6 Výpadek elektřiny

Jelikož budova stojí v průmyslové zóně, může dojít celkem snadno k výpadku elektřiny, důvodů může být několik (tovární hala vedle přetíží síť, vlivem rozšíření průmyslové zóny dělníci překopnou elektrický kabel). Doporučil bych záložní zdroj energie, který pokryje po nějakou dobu výpadku běh serverů. Tady je důležité si stanovit, zda můžou servery důsledkem výpadku elektřiny nějakou kratší dobu nefungovat, myšleno do jedné hodiny. Jestli ano, nemá smysl záložní zdroj pořizovat, jelikož jeho finanční nákladnost je vysoká. Pokud u nás někdo hostuje server s podmínkou, že server musí běžet takzvaně 24/7 365 dní v roce, tak bych nad tím uvažoval, jelikož případné pokuty za nedodržení poskytovaných služeb a způsobené ztráty mohou být poměrně vysoké.

3.7 Požár

Mít všude v budově detektory kouře a protipožární dveře minimálně v serverovně. V případě požáru ve vedlejší místnosti dokážou zachránit celou serverovnu a vy předejte případné velké finanční ztrátě. Sice počáteční investice je větší, ale vzhledem k případně ztrátě je zanedbatelná, tudíž bych do protipožárních prvků investoval.

3.8 Výpadek internetu

Výpadek internetu většinou přijde nečekaně, často to bývá způsobené tím, že dělníci překopnou kabel. Důležité je mít s poskytovatelem internetu domluvu, jak v takových případech postupovat.

4 Závěr

Cílem semestrálního projektu bylo vytvořit případovou studii analýzy rizik ve firmě Bosting, která provozuje datacentrum. Snažil jsem se firmu analyzovat, najít případné bezpečnostní problémy a rizika, která by mohly firmu poškodit.

Firma Bosting však měla dobře nastavená interní pravidla a bezpečnostní politiku, ale i tak se objevili určité nedostatky. Nedostatky jsem analyzoval a následně jsem sepsal opatření, které by mohla firma implementovat, aby eliminovala případné bezpečnostní problémy a rizika.