BOIT

CHECKLIST IT BEZPEČNOSTI

CHECKLIST IT BEZPEČNOSTI

UŽIVATELSKÁ IDENTITA

1. Nepoužíváme služby zdarma a soukromé účty k pracovním účelům (Seznam mail, Gmail, apod.). ☐
2. Nemáme jeden společný účet pro všechny uživatele (uživatelský účet, Gmail, Dropbox, apod.). ☐
3. Používáme centrální systém správy identit (Active directory, AzureAD, OpenLDAP, apod.). ☐
4. Zaměstnanci se nepřipojují k free Wi-Fi na veřejných místech, mají zřízenou VPN. ☐
5. Pro hosty je vyčleněna speciální Wi-Fi síť, bez prostupů do té firemní. ☐
6. Zaměstnanci nepoužívají soukromé účty pro pracovní účely a naopak, stejně tak hesla. ☐
7. Minimálně klíčové účty mají nastaveno multifaktorové ověřování (Aplikace, SMS,..) pro přístup ke službám dostupným z internetu. ☐
8. Zaměstnanci mají vytvořené firemní účty pro přístup do interních a produkčních informačních systémů, nepoužívají soukromé účty. ☐

CHECKLIST IT BEZPEČNOSTI

ZAŘÍZENÍ UŽIVATELŮ

1. Disky notebooků, stanic a mobilních zařízení jsou šifrované. ☐
2. Používáme centrální systémy správy zařízení, jak pro počítače, tak MDM pro mobilní telefony. ☐
3. Vynucujeme automatické zamknutí zařízení – počítačů i mobilů. Uživatelé znají a používají zkratku Win+L. ☐
4. Centrálně řídíme aktualizace operačního systému i aplikací. ☐
5. Firmware zařízení je pravidelně aktualizován, EFI a BIOS jsou chráněny hesly. ☐
6. Operační systém je naistalován z důvěryhodného zdroje a v 64-bit verzi. ☐
7. Používáme antivirové řešení, které centrálně spravujeme a dohledujeme. ☐
8. BYOD – Zaměstnanci nepoužívají soukromá zařízení pro pracovní účely, protože soukromá zařízení nejsou pod správou organizace. ☐
9. Blokujeme neznámé USB disky – ideální stav je povolit připojení jen povolených flešek (dle sériových čísel). ☐
10. Pokud není možné zavést blokaci neznámých USB, tak vynucujeme antivirovou kontrolu připojených zařízení. ☐
11. Kontrolujeme omezení přístupu zařízení (kamer, tiskáren apod) k internetu, pokud to nevyžaduji ke své funkci. ☐
12. Automaticky blokujeme zařízení, které vykazuje známky podezřelé aktivity. ☐

CHECKLIST IT BEZPEČNOSTI

HESLA A PHISHING

1. Zaměstnanci i management jsou poučeni o problematice tvorby a úniků hesel. ☐
2. Používáme dostatečně silná a unikátní hesla pro každý systém, účet a službu. ☐
3. Hesla nemáme připíchnutá na nástěnkách, lepících na monitorech či v Excelech na Ploše. ☐
4. Používáme správce hesel mimo internetový prohlížeč a máme do něj opravdu silné heslo – frázi. ☐
5. Pro přístup ke klíčovým systémům (O365, G-suite) používáme multifaktorové ověření. ☐
6. Pomocí politik vynucujeme komplexnost hesel, ale zbytečně uživatele nezatěžujeme. ☐
7. Zaměstnanci prošli školením, jak rozpoznat phishing a jak s ním nakládat. ☐
8. Školení IT bezpečnosti dostává každý nový zaměstnanec a školení pro všechny pravidelně aktualizujeme a opakujeme. ☐
9. Testujeme své zaměstnance pomocí simulovaných phishingových útoků. ☐
10. Zaměstnanci i management byli poučeni o technikách sociálního inženýrství a jsou proti nim imunní. ☐

CHECKLIST IT BEZPEČNOSTI

PRIVILEGOVANÉ ÚČTY A KONTROLA ADMINISTRÁTORŮ

1. Pro běžnou práci používáme uživatelské účty bez administrátorských oprávnění. ☐
2. Administrátor sám používá privilegovaný účet jen v nutných případech, jinak pracuje také pod uživatelským účtem. ☐
3. Uživatelé ani vedoucí pracovníci nemají práva administrátora. ☐
4. Dodržujeme princip „Least privilege“ – tedy používáme co možná nejnižší oprávnění, která potřebujeme. ☐
5. Máme zapnuté audit logy a zaznamenáváme vše, co který administrátor udělal. ☐
6. IT oddělení pravidelně testuje Disaster Recovery plán, včetně scénářů pro ransomware útok, či živelnou pohromu. ☐
7. Administrátoři nepoužívají k přihlášení k uživatelským stanicím účty s vysokým oprávněním ale servisní, nebo jen dočasné účty. ☐
8. Máme zřízen záložní přístup do všech systémů a ten je bezpečně uložen, třeba v obálce v trezoru. ☐
9. IT vede dokumentaci k projektům a implementacím, aby bylo jasné, co, a jak bylo provedeno. ☐
10. Počítáme s možností odchodu IT pracovníka a nejsme na něm plně závislí. ☐
11. Máme připraven scénář pro resetování administrátorových účtů a zamezení jeho přístupu do organizace. ☐

CHECKLIST IT BEZPEČNOSTI

AKTUALIZACE / SERVERY A HOSTING

1	Nemáme do internetu publikované přihlašování přes RDP (vzdálenou plochu) či jiných interních systémů.	☐
2	Pravidelně aktualizujeme nejen serverové operační systémy, ale i služby a další programy.	☐
3	Nepoužíváme „portable“ verze programů.	☐
4	Máme nasazen firewall a kontrolujeme jeho provoz.	☐
5	Používáme systém na centrální sběr logů (SIEM).	☐
6	Provádíme inspekci provozu a pravidelně sledujeme reporty, máme nastaveny notifikace na zvláštní události.	☐
7	Firemní síť je segmentovaná – rozdělena do samostatných částí, které nemusí být nutně vzájemně prostupné.	☐
8	Máme izolovaný provoz v podsítích pro zaměstnance/hosty a samostatný subnet pro chytrá zařízení, IoT, a podobně.	☐
9	Máme zajištěnou fyzickou bezpečnost serverovny.	☐
10	Volně dostupná zařízení jako jsou kiosky mají zaslepené USB porty a jsou zaplombovány.	☐
11	Poskytovatel hostingu má bezpečnostní audit, pravidelně záplatuje a zálohuje a je schopný to doložit	☐
12	Automaticky blokujeme naši IP proti útokům hrubou silou.	☐

CHECKLIST IT BEZPEČNOSTI

FIREMNÍ WEBY A SOCIÁLNÍ SÍTĚ

1. Weby běží na HTTPS i když na nich není možnost se přihlásit k firemním systémům ☐
2. Služby, ke kterým se přihlašují jak zaměstnanci i IT pracovníci, mají vždy platný a podepsaný certifikát. ☐
3. Firemní weby neobsahují zranitelnosti. ☐
4. Na webu nejsou informace v rozporu s GDPR a fotografie a osobní údaje zaměstnanců, záznamy z kamerových systémů a pod. ☐
5. Na sociálních sítích máme oficiální profil firmy, který má několik správců a moderátorů. ☐
6. Zaměstnanci nezakládají na sociálních sítích neveřejné firemní skupiny a nesdílejí interní data přes messengery. ☐
7. Pro komunikaci se zákazníky existuje jednotný komunikační kanál či agregátor. ☐
8. Při pořádání webinářů se řídíme doporučenými bezpečnostními postupy. ☐

CHECKLIST IT BEZPEČNOSTI

ZÁLOHOVÁNÍ DAT

1. Automaticky a v pravidelných intervalech zálohujeme důležitá data - servery, interní systémy, data uživatelů, … ☐
2. Dodržujeme pravidlo 3-2-1. Zálohujeme 3 kopie dat, na 2 rozdílné typy úložišť a 1 kopii ukládáme fyzicky mimo firmu. ☐
3. Máme připraven Disaster Recovery plán – plán obnovy po havárii či útoku a ten alespoň jednou ročně testujeme. ☐
4. Pravidelně testujeme obnovu a konzistenci záloh, i když vše funguje. ☐
5. Máme zálohy zabezpečeny a odděleny pro případ útoku. ☐

Gratulujeme k dokončení kontroly.

Nyní doporučujeme seřadit nesplněné body dle závažnosti a začít s jejich odstraňováním.

Nevíte si rady? Proto jsme tu my.

https://boit.cz