GORDIC

10 „P“ kybernetické bezpečnosti

aneb preventivní kroky pro rychlou pomoc

1. Pravidelná školení, cvičení a systematické vzdělávání personálu a managementu
2. Přívětivá a dostupná osvěta pro personál a management
3. Proaktivní studium a využívání odborných i osvětových portálů, médií a konferencí
4. Profesionální ICT personál a management
5. Povinná nebo přiměřená realizace opatření vyplývajících ze Zákona o kybernetické bezpečnosti (ZKB)
6. Praktikování zavedení a udržování systému bezpečnosti informací (ISMS)
7. Permanentní zlepšování kybernetické bezpečnosti a jeho systematické řízení (CSA)
8. Používání a pravidelná údržba a aktualizace bezpečného systémového, bezpečnostního a aplikačního programového a technického vybavení
9. Pravidelné a bezpečné zálohy všech dat, ukládané odděleně od vlastní sítě
10. Preventivní a rychlá realizace ověřených a doporučených praktik

„Největším nebezpečím pro kybernetickou bezpečnost jsou lidé, jejich šéfové a potom až technologie a internet.“

Ing. Michal Řezáč MSc.

ředitel platformy KYBEZ

10 „P“ kybernetické bezpečnosti

aneb preventivní kroky pro rychlou pomoc

1. Pravidelná školení, cvičení a systematické vzdělávání personálu a managementu

Školení, cvičení i řízený proces systematického vzdělávání personálu a managementu (včetně prověřování úrovně odolnosti proti phishingu a využití dalších nástrojů) v oblasti kyberbezpečnosti je, jak se zas a znovu ukazuje, neodmyslitelná součást funkčního řízení organizace jakéhokoliv typu a rozměru. I nejlepší antivir a firewall v počítači postrádají smysl, když za klávesnicí sedí nezodpovědný či nevzdělaný pracovník. Smysluplné řízení vzdělávání je dlouhodobý a nikdy nekončící proces.

2. Přívětivá a dostupná osvěta pro personál a management

Na první krok navazuje i nutnost dostupnosti a srozumitelnosti vzdělávání. Kybernetická bezpečnost není pro každého snadno pochopitelné téma. Kromě závěrů z dřívějších krizových simulací a dalších forem ověření úrovně znalostí je nutné i tento aspekt při nastavování vzdělávacího procesu vždy reflektovat. Každý pracovník musí mít dostupné pro něj relevantní informace, které mu jsou předávány stylem, jakému rozumí. Pouhý přepis nabiflovaných odpovědí ze skript do testu ke zlepšení zabezpečení nevede.

3. Proaktivní studium a využívání odborných i osvětových portálů, médií a konferencí

Dynamika hackerského vývoje počítačových virů a škodlivých procesů či technologií je obrovská a to, jakým směrem se tyto hrozby v budoucnu posunou, lze jen stěží odhadovat. Tematiku kybernetické bezpečnosti je tak nutné neustále sledovat a proaktivně přistupovat k jejímu studiu. K tomu dokáže organizacím pomoci řada odborných i osvětových portálů, médií i konferencí. K systematické a dlouhodobé osvětě a vzdělávání ve sféře kybernetické bezpečnosti přispívá i platforma KYBEZ (www.kybez.cz).

4. Profesionální ICT personál a management

Jistě, určitou míru znalostí v oblasti kybernetické bezpečnosti by měli mít všichni zaměstnanci i manažeři. Nutné je však i disponovat (ať už interními nebo externími) pracovníky s vysokou ICT odborností, zaručenou zastupitelností a podporou aktivně zapojeného vrcholového managementu. Pouze tak lze zajistit nepřetržitou možnost okamžitého řešení sporných či krizových situací. GORDIC (www.gordic.cz) poskytuje řadě organizací veřejné správy i soukromého sektoru odborné kapacity profesionálů v oblasti ICT.

5. Povinná nebo přiměřená realizace opatření vyplývajících ze Zákona o kybernetické bezpečnosti (ZKB)

O tomto bodě snad ani nemůže být pochyb. Zároveň platí, že neznalost norem neomlouvá, proto je třeba vědět, jaká je pro konkrétní organizaci relevantní legislativa a do jaké míry pro ni platí povinnost souladu s jednotlivými články Zákona o kybernetické bezpečnosti, Vyhlášky o kybernetické bezpečnosti, legislativy řešící ochranu osobních údajů (GDPR, ...) a dalších norem. I zde platí, že právo je minimem morálky - pro organizace, které v tematice kyberbezpečnosti tápou, však zároveň i dobrým odrazovým můstkem.

6. Praktikování zavedení a udržování systému bezpečnosti informací (ISMS)

Nejen zavést, ale i dlouhodobě udržovat Systém řízení bezpečnosti informací je opatřením, které organizacím dovede zajistit ochranu informačních aktiv a důsledné řízení rizik z kategorie bezpečnosti informací. Zodpovědný přístup by měl organizaci dovést k eliminaci možných ztrát informací i jejich jakéhokoliv poškození. Metodicky správné systémové řízení bezpečnosti informací patří k základním stavebním kamenům kybernetického zabezpečení. Dosavadní bezproblémový chod není zárukou klidné budoucnosti.

7. Permanentní zlepšování kybernetické bezpečnosti a jeho systematické řízení (CSA)

Správné nastavení systému řízení kybernetické bezpečnosti netrvá pouze do vytištění první analýzy rizik, jde o nekončící cyklický proces s řadou nutností – od ocenění bezpečnostních aktiv, identifikace, hodnocení a řízení rizik přes řešení aplikovatelnosti opatření a plán zvládání rizik až po audit kyberbezpečnosti. Vše samozřejmě musí reflektovat aktuální legislativu i specifika organizace. Naštěstí existuje částečně automatizované řešení - nástroj CSA platformy Gordic CyberSec (www.gordiccybersec.cz).

8. Používání a pravidelná údržba a aktualizace bezpečného systémového, bezpečnostního a aplikačního programového a technického vybavení

Kromě lidských a procesních cest musí vést klíčové kroky do kyberbezpečí i přes oblast technologií. Používání a pravidelná údržba a aktualizace bezpečného systémového, bezpečnostního a aplikačního programového a technického vybavení tvoří další klíčový díl do mozaiky zodpovědné prevence. Nutné je i zavádění technických opatření navazujících na směrnice a politiky vymezující správné chování. Jako příklady lze uvést segmentaci vnitřní sítě, pravidelné skeny zranitelností, monitoring nebo šifrování.

9. Pravidelné a bezpečné zálohy všech dat, ukládané odděleně od vlastní sítě

Prevence samozřejmě neznamená jenom předcházení možným hrozbám – ostatně ztráta dat může přijít i kvůli omylu pracovníka či selhání HW. A co si budeme nalhávat, hackeři bývají také čas od času o krok napřed a prolomí i důstojnou kybernetickou obranu (vinou člověka, procesu či technologie). Za nutnost tak lze považovat i opatření, která minimalizují dopady takových hrozeb. Konkrétně jde o důsledné, pravidelné a nejlépe automatické zálohování, ideálně včetně cvičného obnovení záloh.

10. Preventivní a rychlá realizace ověřených a doporučených praktik

Rychlá realizace ověřených a doporučených praktik není nikdy na škodu. Inspirovat se tím, co funguje jinde, je zcela logické a správné opatření – samozřejmě s ohledem na specifika konkrétní organizace. Pozitivním pro firmy i subjekty veřejné správy je fakt, že existují společnosti i orgány (NÚKIB, NCKB, CIIRC, KYBEZ, ...), které vydávají a veřejně prezentují soubory doporučených opatření (ať už těch obecně preventivních, nebo reagujících na konkrétní stav).