Stručná metodika workshopu o IT bezpečnosti s názvem

„Jak se (ne)chovat ve firemní síti“

1. **Co se událo v poslední době**
   Seznámení uživatelů s aktuálními tématy z oblasti IT bezpečnosti. V drtivé většině případů se jedná o události, které se objevovaly v médiích. Seznámíme uživatele s podstatou těchto událostí a osvětlíme příčiny a následky.

2. **Počátky škodlivých sw (malware), způsob jejich šíření a dopady**
   V této kapitole zmapujeme historický vývoj (evoluce) škodlivého software od dob prvních osobních počítačů. Rozebereme způsoby šíření, typické formy útoků a jejich cíle. Na dobových příkladech ukážeme nejzajímavější události.

3. **Rozdělení malware...co je to virus, červ, trojan, spyware,…**
   Vysvětlení pojmu „malware“ a jeho základní rozdělení podle kategorií. Ke každé kategorii je uvedeno několik příkladů a bližší informace, jak se proti danému typu útoku chránit.

4. **Nové formy útoků s rozvojem internetu a mobilních technologií**
   Rozbor nových forem útoku v návaznosti na rozvoj webových aplikací, mobilních zařízení a přesunu dat do cloudů. Zvláštní pozornost je věnována podvodným aplikacím pro mobilní platformy. Na závěr této kapitoly je připravena praktická ukázka krádeže přihlašovacích údajů.

5. **Hackeři, crackeři a hacktivisti…jejich původ, charakteristika, motivace a nebezpečnost**
   Seznámení uživatelů s pojmem „hacker“, jeho mutacemi a hacktivistickými skupinami. Původ a vývoj hackerů a hackerských skupin, jejich motivace a společenská nebezpečnost. Typické příklady hackerských útoků a jejich dopady na firemní i státní infrastruktury. Zmíníme možnosti pokročilé autentizace do firemní sítě (SecurID, 802.1x)
   Závěr kapitoly je věnován praktické ukázce zabezpečení Wi-Fi.

6. **Proč je neznalý zaměstnanec největší hrozbou pro podnikovou síť a co riskuje (příklady zaměstnaneckých selhání)**
   Seznámení zaměstnanců s riziky, která jsou spojena s charakterem jejich činnosti ve firemní síti. Vysvětlení hrozeb a jejich následků plynoucích z neopatrnosti a neuvědomělého jednání. Ukázky a příklady úniků citlivých dat, které způsobili neopatrní zaměstnanci.

7. **Jak nejčastěji unikají firemní data a jak je chránit**
   Rozbor možných způsobů, jak mohou z firem unikat citlivá data. Důraz je kladen zejména na úniky spojené s běžnou kancelářskou prací na PC. Součástí této kapitoly je praktická ukázka

šifrování dat na úrovni Microsoft EFS i produktů třetích stran. Vysvětlíme základní principy symetrického a asymetrického šifrování.

8. **Certifikáty a digitální podpisy**
   Rozebereme problematiku elektronických certifikátů, certifikačních autorit a jejich praktické použití. Pro osobní i firemní využití seznámíme uživatele také s problematikou digitálních podpisů. Seznámíme uživatele s problémy zcizených kořenových certifikátů.

9. **(Ne)bezpečná komunikace**
   Kapitola je věnována principům elektronické komunikace. Zaměříme se zejména na bezpečnost e-mailů a protokolu HTTP/S. Součástí této kapitoly je praktická ukázka krádeže dat pomocí „keyloggeru“.

10. **Něco málo z legislativy ČR**
    Okrajově seznámení se zákonem č. 412/2005 o ochraně utajovaných informací a návrhem zákona o kybernetické bezpečnosti.

11. **Důležitost správně zvoleného hesla a jeho ochrana, praktický návod, jak zvolit silné heslo**
    Uživatelé zpravidla opomíjejí praktiky pro vytváření silných hesel, nebo je vůbec neznají. V této kapitole se zaměstnanci naučí vytvářet silná hesla s pomocí osvědčených praktik.

12. **Jak bezpečně zacházet s mobilním zařízením (smart phone, tablet, notebook,…)**
    Mobilní platformy jsou dnes běžnou součástí firemních sítí a mnoho firem vyznává politiku BYOD. Díky jejich stále rostoucí popularitě se množí i cílené útoky na tyto platformy. Tato kapitola se věnuje bezpečnému zacházení s těmito zařízeními a možnostmi ochrany.

13. **Stahování a šíření digitálního obsahu vs. autorský zákon**
    Uživatelé mají tendenci instalovat na svěřené IT technologie nelegální software a kopírovat nelegální obsah. Bohužel riziko nese v tomto případě zaměstnavatel, jakožto vlastník/provozovatel. V této kapitole vysvětlujeme zaměstnancům právní aspekty a dopady takového chování.

14. **Útok formou „sociálního inženýrství“**
    Vysvětlení pojmu „sociální inženýrství“, jakožto novodobé hrozby pro firemní data. Zdůraznění jeho společenské nebezpečnosti a vlivu. Nástin možných scénářů napadení běžného zaměstnance, rozpoznání útoku a způsob obrany.

15. **Proč zaměstnavatelé neradi vidí sociální sítě, free maily, chatovací nástroje, atp.**
    V této kapitole získají uživatelé informace o rizicích, která jsou spojená s využíváním webových aplikací, jako jsou e-mailové služby pro veřejnost, sociální sítě, chatovací a komunikační nástroje, sdílená úložiště, atp.

16. **Jak si zabezpečit svůj počítač a data**
    Tato kapitola je věnována zabezpečení domácích stanic uživatelů. Důležité je, aby si zaměstnanci osvojili bezpečnostní praktiky také na domácích stanicích. Bezpečnostní praktiky se musejí stát pro uživatele jakýmsi podmíněným reflexem.

17. **Desatero zásad, které pomůže předejít útokům a ztrátám dat**
    Uživatelům zdůrazníme desítku nejdůležitějších zásad, kterými by se měli řídit, aby tak předešli ztrátě dat a jejich možnému zneužití.

18. **Prostor pro diskuzi**

19. **Závěrečný interaktivní test**

SHIFTCOM s.r.o. – centrála

Prokopova 498

Louny,440 01

e-mail: louny@shiftcom.cz

tel: +420 606 706 856