VIAVIS střežíme podstatné

Chování v kyberprostoru

V úvodu semináře je posluchač seznámen se základními pojmy v oblasti kybernetické bezpečnosti. V dalších částech semináře je posluchač seznamován se základními technikami útoků, se kterými se může setkat, a to jak v osobním životě, tak při výkonu svého povolání, přičemž je kladen důraz na osvětlení této problematiky z pohledu návaznosti na zabezpečení kybernetické bezpečnosti informační a komunikační techniky zaměstnavatele.
Posluchači jsou seznámeni s různými technickými útoky, které využívají současní hackeři a to včetně živých ukázek. Část semináře je také věnován technikám sociálního inženýrství, při které jsou posluchači seznámeni například s aktuální problematikou tzv. phishingových e-mailů. Každá jednotlivá hrozba, která je v průběhu semináře posluchačům představena je následovaná základními bezpečnostními opatřeními, kterými je běžný uživatel schopen eliminovat rizika. Po absolvování semináře je posluchač obeznámen se základní problematikou kybernetické bezpečnosti, je mu známa návaznost jeho rizikového chování v kyberprostoru na infrastrukturu zaměstnavatele a jsou mu známy základní techniky, kterými je schopen omezit rizika.

Cílem semináře je seznámit posluchače se základními hrozbami v kyberprostoru a se zásadami bezpečného chování v kyberprostoru v návaznosti na komplexní zabezpečení firemní infrastruktury. Seminář je určen pro všechny zaměstnance, kteří při výkonu svého povolání přicházejí do styku s informační a výpočetní technikou.

Obsah semináře:

- přehled základních kybernetických hrozeb, se kterými se běžný uživatel může setkat;
- rizika mobilních zařízení a dat, která obsahují přístupy do interní sítě zaměstnavatele;
- ukázky reálných útoků;
- základní bezpečnostní uživatelské návyky;
- diskuse, zodpovězení otázek.

Rozsah semináře:	**4 hodiny**
Počet posluchačů:	**do 20 osob**
Cena semináře:	**20.000 Kč bez DPH, cena s DPH 24.200 Kč**