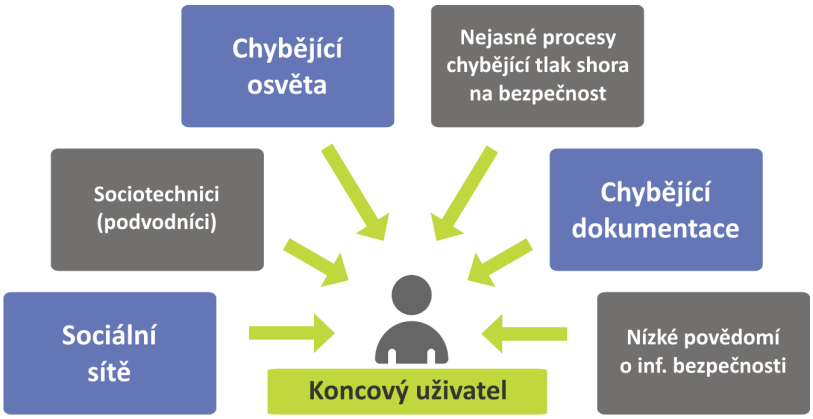
Bezpečnost koncových uživatelů

Bezpečnost koncových uživatelů představuje soubor opatření pro zvýšení bezpečnostní úrovně uživatelů, jako je povědomí o informační bezpečnosti, chování v IS, odpovědnost atd.



Testy metodami sociálního inženýrství

Cílem je přimět testovanou osobu, aby prozradila určitou informaci (typicky login, heslo) nebo vykonala určitou činnost (typicky spustila virus).
Metody:

- E-mailový – testovaným osobám se rozešle e-mail například s vtipy a v příloze je „infikovaný“ soubor s testovacím kódem.
- Telefonický – testovaným osobám se volá pod nejrůznějšími záminkami, např. že jejich PC šíří virus.
- Fyzický – pokusy o průnik do chráněných prostor organizace přes recepci, dveře na kartu apod. Rozšíření “infikovaných” datových médií po prostorách organizace.

Školení informační bezpečnosti:

- Prezentační – přednášky lektora pro různé úrovně znalostí inf. bezpečnosti včetně závěrečného testu.
- E-learning – vývoj aplikací, které zákazník nasadí uvnitř organizace, a každý zaměstnanec se vzdělává sám.

Propagace bezpečnosti:

- Bezpečnostní portál - zpracování podkladů a materiálů pro portál (periodický bulletin obsahující aktuality, plakáty, komiksy, školicí materiály, bezpečnostní dokumentace, odkazy na zajímavé weby).

Přínosy našich služeb

Díky testům metodami sociálního inženýrství a zkoumáním sociálních sítí získá klient reálnou představu, čeho jsou jeho zaměstnanci schopni a jaké představují riziko; získá argumenty pro stanovení bezpečnostních pravidel, například pro školení atp. Již samotná realizace testů zpravidla zvyšuje bezpečnostní povědomí zaměstnanců organizace (stávají se tématem hovoru atd.).

Propagace bezpečnosti, školení inf. bezpečnosti a implementace do bezp. dokumentace přinesou stanovení povinností a odpovědností uživatelů IS organizace. Všichni zaměstnanci budou znát konkrétní odpovědnosti a povinnosti při práci s IS. Zvýší se bezpečnostní povědomí uživatelů o informační bezpečnosti. Sníží se riziko úniku dat, např. prostřednictvím e-mailové komunikace apod. Bude omezena „absolutní moc“ administrátorů a správců. Stoupá význam role bezpečnostního manažera.

Implementace bezpečnostní dokumentace:

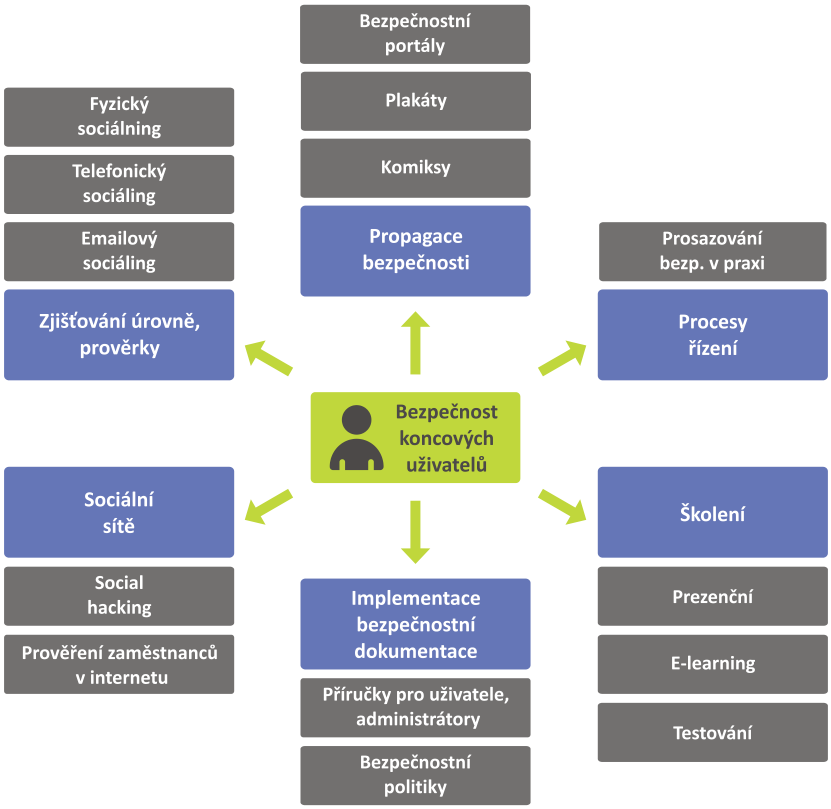
- Bezpečnostní politiky - vytvoření či aktualizace celkové bezpečnostní politiky, systémové BP, atd.
- Vytvoření bezpečnostních příruček pro administrátory, uživatele, bezpečnostní manažery, apod.

Sociální sítě:

- Prověření zaměstnanců – co zveřejňují o organizaci na sociálních sítích.
- Social hacking – sbírání informací o organizaci prostřednictvím falešné identity na sociální síti.

Procesní audity:

- Formou interview jsou identifikovány postupy a bezpečnostní nedostatky procesů, např. životního cyklu bankovního účtu, administrace aplikace apod.



Proč AEC?

Společnost AEC představuje spolehlivého partnera na poli informační bezpečnosti s 20letou tradicí na trhu. Disponuje silným týmem pěti bezpečnostních konzultantů, přičemž každý se specializuje na specifické oblasti. AEC může nabídnout zkušenosti získané dlouholetou praxí. Důvěru nám dávají velké firmy i menší organizace.

Reference

- ING Management Services, s.r.o.
- Komerční pojišťovna, a.s.
- ČEZ ENERGOSERVIS, spol. s r.o.
- Ministerstvo práce a sociálních věcí ČR
- Městský úřad Tábor

AEC, spol. s r.o.
Purkyňova 2845/101
612 00 Brno, Czech Republic
Phone: +420 530 507 200
Fax: +420 530 507 220

AEC, spol. s r.o.
European Business Center
Dukelských hrdinů 34
170 00 Praha 7, Czech Republic
Phone: +420 267 311 402
Fax: +420 266 177 155

AEC
DATA SECURITY

www.aec.cz