

Odborný zamestnanec

Rola:	Odborný zamestnanec																																		
Vedomosti:	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%;">1) vybrané základné pojmy v kybernetickej bezpečnosti</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>2) význam osobných údajov a citlivých informačných aktív</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>3) zdroje typických hrozieb a kategórie hrozieb (úmyselné hrozby, náhodné hrozby, hrozby prostredia)</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>4) aktuálne typy hrozieb (napr. škodlivý kód, phishing, spam, útok na internetové služby alebo stránky (Denial of Service (DoS)/znemožnenie prístupu k požadovanej službe (Distributed denial of service (DDoS), botnety, krádež identity a ďalšie)</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>5) identifikácia, autentizácia, autorizácia</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>6) spôsoby overenia digitálnej totožnosti význam viacfaktorovej autentizácie a typy autentizačných faktorov</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>7) základné princípy bezpečného používania hesiel</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>8) význam škodlivého kódu (malvér) a spôsoby útokov škodlivým kódom</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>9) riziká používania zariadení IKT</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>10) základné zraniteľnosti smartfónov</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>11) základné princípy vzdialeného prístupu a bezpečnostné zásady pri práci na diaľku</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>12) obsah pojmu digitálne súkromie</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>13) význam pojmov digitálny podpis, elektronický podpis, kvalifikovaný elektronický podpis, časová pečiatka</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>14) základné zásady bezpečnosti, ochrany osobných údajov a etikety pri telekonferenciách a online rokovaníach, stretnutiach</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>15) bezpečnostné riziká a riziká ochrany súkromia pri používaní sociálnych sietí pokiaľ sú v organizácii povolené</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>16) podstata útokov formou sociálneho inžinierstva (phishing, vishing, smishing, Business Email Compromise)</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> <tr> <td>17) základné poznatky na úseku trestného práva</td> <td style="text-align: right; vertical-align: top;">BL2</td> </tr> </table>	1) vybrané základné pojmy v kybernetickej bezpečnosti	BL2	2) význam osobných údajov a citlivých informačných aktív	BL2	3) zdroje typických hrozieb a kategórie hrozieb (úmyselné hrozby, náhodné hrozby, hrozby prostredia)	BL2	4) aktuálne typy hrozieb (napr. škodlivý kód, phishing, spam, útok na internetové služby alebo stránky (Denial of Service (DoS)/znemožnenie prístupu k požadovanej službe (Distributed denial of service (DDoS), botnety, krádež identity a ďalšie)	BL2	5) identifikácia, autentizácia, autorizácia	BL2	6) spôsoby overenia digitálnej totožnosti význam viacfaktorovej autentizácie a typy autentizačných faktorov	BL2	7) základné princípy bezpečného používania hesiel	BL2	8) význam škodlivého kódu (malvér) a spôsoby útokov škodlivým kódom	BL2	9) riziká používania zariadení IKT	BL2	10) základné zraniteľnosti smartfónov	BL2	11) základné princípy vzdialeného prístupu a bezpečnostné zásady pri práci na diaľku	BL2	12) obsah pojmu digitálne súkromie	BL2	13) význam pojmov digitálny podpis, elektronický podpis, kvalifikovaný elektronický podpis, časová pečiatka	BL2	14) základné zásady bezpečnosti, ochrany osobných údajov a etikety pri telekonferenciách a online rokovaníach, stretnutiach	BL2	15) bezpečnostné riziká a riziká ochrany súkromia pri používaní sociálnych sietí pokiaľ sú v organizácii povolené	BL2	16) podstata útokov formou sociálneho inžinierstva (phishing, vishing, smishing, Business Email Compromise)	BL2	17) základné poznatky na úseku trestného práva	BL2
1) vybrané základné pojmy v kybernetickej bezpečnosti	BL2																																		
2) význam osobných údajov a citlivých informačných aktív	BL2																																		
3) zdroje typických hrozieb a kategórie hrozieb (úmyselné hrozby, náhodné hrozby, hrozby prostredia)	BL2																																		
4) aktuálne typy hrozieb (napr. škodlivý kód, phishing, spam, útok na internetové služby alebo stránky (Denial of Service (DoS)/znemožnenie prístupu k požadovanej službe (Distributed denial of service (DDoS), botnety, krádež identity a ďalšie)	BL2																																		
5) identifikácia, autentizácia, autorizácia	BL2																																		
6) spôsoby overenia digitálnej totožnosti význam viacfaktorovej autentizácie a typy autentizačných faktorov	BL2																																		
7) základné princípy bezpečného používania hesiel	BL2																																		
8) význam škodlivého kódu (malvér) a spôsoby útokov škodlivým kódom	BL2																																		
9) riziká používania zariadení IKT	BL2																																		
10) základné zraniteľnosti smartfónov	BL2																																		
11) základné princípy vzdialeného prístupu a bezpečnostné zásady pri práci na diaľku	BL2																																		
12) obsah pojmu digitálne súkromie	BL2																																		
13) význam pojmov digitálny podpis, elektronický podpis, kvalifikovaný elektronický podpis, časová pečiatka	BL2																																		
14) základné zásady bezpečnosti, ochrany osobných údajov a etikety pri telekonferenciách a online rokovaníach, stretnutiach	BL2																																		
15) bezpečnostné riziká a riziká ochrany súkromia pri používaní sociálnych sietí pokiaľ sú v organizácii povolené	BL2																																		
16) podstata útokov formou sociálneho inžinierstva (phishing, vishing, smishing, Business Email Compromise)	BL2																																		
17) základné poznatky na úseku trestného práva	BL2																																		
Zručnosti:	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%;">1) bezpečná manipulácia s prostriedkami IKT, osobnými údajmi a citlivými informačnými aktívami</td> </tr> <tr> <td>2) používanie stanovených bezpečnostných mechanizmov v pracovných procesoch</td> </tr> <tr> <td>3) rozpoznanie bezpečnostného incidentu a schopnosť správne reagovať na incident</td> </tr> <tr> <td>4) dodržiavanie bezpečnostných zásad a platných politík</td> </tr> </table>	1) bezpečná manipulácia s prostriedkami IKT, osobnými údajmi a citlivými informačnými aktívami	2) používanie stanovených bezpečnostných mechanizmov v pracovných procesoch	3) rozpoznanie bezpečnostného incidentu a schopnosť správne reagovať na incident	4) dodržiavanie bezpečnostných zásad a platných politík																														
1) bezpečná manipulácia s prostriedkami IKT, osobnými údajmi a citlivými informačnými aktívami																																			
2) používanie stanovených bezpečnostných mechanizmov v pracovných procesoch																																			
3) rozpoznanie bezpečnostného incidentu a schopnosť správne reagovať na incident																																			
4) dodržiavanie bezpečnostných zásad a platných politík																																			