# **SIGURIA KIBERNETIKE DHE MENAXHIMI I INCIDENTEVE**

|  |
| --- |
| **Moduli me pak fjalë** |
| Nxënësit mësojnë kërcënimet dhe dobësitë e sigurisë kibernetike, metodat e përdorura për të mbrojtur sistemet nga kërcënimet dhe si të planifikojnë dhe menaxhojnë incidentet e sigurisë. |
| **Prezantimi i modulit** |
| Mbështetja jonë në rritje në sistemet kompjuterike dhe të dhënat që ato përmbajnë na bën të prekshëm ndaj sulmeve nga kriminelët kibernetikë dhe ndaj humbjes së këtyre sistemeve nëse ka një aksident ose një fatkeqësi natyrore. Me përmirësimin e sigurisë së sistemit të TI-së, zhvillohen metoda më të sofistikuara të sulmit dhe është e rëndësishme që organizatat të kenë plane të forta për t'u marrë me një incident të sigurisë kibernetike përpara se të ndodhë. Të gjithë profesionistët e TI-së kërkojnë një kuptim të mirë të kërcënimeve aktuale ndaj sistemeve, si të aplikojnë metoda të përshtatshme dhe efektive të mbrojtjes dhe si të menaxhojnë një incident të sigurisë kibernetike.  Vendet në mbarë botën po përshpejtojnë përpjekjet për të adresuar rreziqet e sigurisë kibernetike ndaj rrjeteve të tyre të komunikimit të sigurisë publike dhe misionit kritik. Në këtë njësi, ju do të shqyrtoni shumë lloje të ndryshme të sulmeve të sigurisë kibernetike, dobësitë që ekzistojnë në sistemet e rrjetit dhe teknikat që mund të përdoren për të mbrojtur sistemet e rrjetit të një organizate. Ju do të hulumtoni teknikat e përdorura për të vlerësuar rreziqet dhe mënyrat e planifikimit për t'u marrë me rezultatet e një incidenti të sigurisë kibernetike dhe për të rikuperuar sistemet pas një incidenti. Ju do të shqyrtoni skenarë, do të kryeni vlerësime të rrezikut dhe përgatitni plane mbrojtëse përpara se të mbroni sistemet e rrjetit. Ju gjithashtu do të shqyrtoni provat nga incidentet e sigurisë kibernetike dhe dokumentacionin përkatës të sigurisë, duke përdorur provat për të bërë rekomandime për përmirësim. Ndërsa sistemet e TI-së evoluojnë, ka një nevojë në rritje për profesionistët e TI-së për të mbrojtur sistemet e rrjetit dhe informacionin që ato përmbajnë, duke ofruar veçori dhe përfitime të përmirësuara për organizatat, klientët dhe individët. |
| **Rezultatet e mësimnxënies 1 (RM1): Nxënësi kupton kërcënimet e sigurisë kibernetike, dobësitë e sistemit dhe metodat e mbrojtjes së sigurisë** |
| **RM1-1 Kërcënimet e sigurisë kibernetike** |
| **RM1-2 Dobësitë e sistemit** |
| **RM1-3 Përgjegjësitë ligjore** |
| **RM1-4 Masat e sigurisë fizike** |
| **RM1-5 Masat e sigurisë së softuerit dhe harduerit** |

|  |  |  |
| --- | --- | --- |
| **Kriteret e vlerësimit (performancës), njohuritë, shkathtësitë dhe kompetencat për RM1** | | |
| Kalon (K) | Me meritë (M) | i/e Dalluar (D) |
| **RM1.K1** Shpjegoni kërcënimet e ndryshme të sigurisë kibernetike që mund të ndikojnë në sistemet e IT të organizatave.  **RM1.K2** Shpjegoni dobësitë e sistemit që mund të ndikojnë në sistemet e IT të organizatave.  **RM1.K3** Shpjegoni se si organizatat mund të përdorin masat e sigurisë fizike, softuerike dhe harduerike për të luftuar kërcënimet e sigurisë. | **RM1.M1** Vlerësoni ndikimin që kërcënimet e sigurisë kibernetike mund të kenë në sistemet e TI-së të organizatave, duke marrë parasysh kërkesat ligjore. | **RM1.RM2.D1** Vlerësoni efektivitetin e masave të përdorura për të mbrojtur organizatat nga kërcënimet e sigurisë kibernetike duke marrë parasysh kërkesat ligjore. |

|  |
| --- |
| **Rezultatet e mësimnxënies 2 (RM2): Nxënësi hulumton** **implikimet e sigurisë të sistemeve në rrjet** |
| **RM2-1 Llojet e rrjetit** |
| **RM2-2 Komponentët e rrjetit** |
| **RM2-3 Shërbimet dhe burimet e infrastrukturës së rrjetëzimit** |

|  |  |  |
| --- | --- | --- |
| **Kriteret e vlerësimit (performancës), njohuritë, shkathtësitë dhe kompetencat për RM2** | | |
| Kalon (K) | Me meritë (M) | i/e Dalluar (D) |
| **RM2.K4** Shpjegoni se si mund të sigurohen llojet dhe komponentet e ndryshëm të rrjetit.  **RM2.K5** Shpjegoni se si siguria kibernetike ndikon në infrastrukturën dhe burimet e rrjetit. | **RM2.M2** Analizoni implikimet e sigurisë të sistemeve të ndryshme në rrjet. | **RM1.RM2.D1** Vlerësoni efektivitetin e masave të përdorura për të mbrojtur organizatat nga kërcënimet e sigurisë kibernetike duke marrë parasysh kërkesat ligjore. |

|  |
| --- |
| **Rezultatet e mësimnxënies 3 (RM3): Nxënësi zhvillon një plan të mbrojtjes së sigurisë kibernetike për një organizatë të caktuar** |
| **RM3-1 Vlerësimi i dobësive të sistemit kompjuterik** |
| **RM3-2 Vlerësimi i ashpërsisë së rrezikut për çdo kërcënim** |
| **RM3-3 Plani për siguri kibernetike për një sistem** |
| **RM3-4 Politikat e brendshme** |
| **RM3-5 Ofruesit e shërbimeve të jashtme** |

|  |  |  |
| --- | --- | --- |
| **Kriteret e vlerësimit (performancës), njohuritë, shkathtësitë dhe kompetencat për RM3** | | |
| Kalon (K) | Me meritë (M) | i/e Dalluar (D) |
| **RM3.K6** Kryerja e një vlerësimi të rrezikut të dobësive të sistemit.  **RM3.K7** Krijoni një plan sigurie kibernetike për sistemin IT të një organizate. | **RM3.M3** Arsyetoni zgjedhjen e masave të sigurisë që përdoren për të mbrojtur sistemet e IT të një organizate. | **RM3.RM4.D2** Vlerësoni planin e sigurisë kibernetike, duke përfshirë ndikimin e tij në politikat e brendshme dhe ofruesit e shërbimeve të jashtme. |

|  |
| --- |
| **Rezultatet e mësimnxënies 4 (RM4): Nxënësi do të shqyrtoj procedurat për të mbledhur prova mjeko-ligjore pas një incidenti sigurie** |
| **RM4-1 Mbledhja e provave mjeko-ligjore** |
| **RM4-1 Analiza sistematike mjeko-ligjore e një sistemi të dyshuar** |

|  |  |  |
| --- | --- | --- |
| **Kriteret e vlerësimit (performancës), njohuritë, shkathtësitë dhe kompetencat për RM4** | | |
| Kalon (K) | Me meritë (M) | i/e Dalluar (D) |
| **RM4.K8** Shpjegoni procedurat mjekoligjore për mbledhjen e provave pas një incidenti sigurie. | **RM4.M4** Analizoni se si zbatohen procedurat mjeko-ligjore në një sistem të dyshimtë. | **RM3.RM4.D2** Vlerësoni planin e sigurisë kibernetike, duke përfshirë ndikimin e tij në politikat e brendshme dhe ofruesit e shërbimeve të jashtme. |