Menaxhimi i Rrezikut Kibernetik

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Tetor, 2024

- ***Webinar “Menaxhimi i Rrezikut Kibernetik” është dizenjuar për një përfshirje dhe pjesëmarrje të gjerë dhe është treguar kujdes i shtuar (përvec se aty kur nuk ka qenë e mundur) në përdorimin e termave teknikë për garantimin e komoditetit të pjesëmarrësve jo të fushës së sigurisë kibernetike.***

- ***Shembujt e marrë në konsideratë, nuk duhet të shihen si shteruese, por si disa nga alternativat më të përdorura gjerësisht për të cilat përdorimi i tyre ka qenë efektiv në situatat e duhura.***

- Peisazhi i rrezikut kibernetik - 2024
- Kornizat ndërkombëtare të menaxhimit të rrezikut kibernetik
- Cikli (Etapat) e Menaxhimit të Rrezikut Kibernetik (Identifikimi, Vlerësimi, Mitigimi dhe Monitorimi)
- Menaxhimi i Rrezikut Kibernetik në Nivel Kombëtar - AKSK

*“…Ai që e njeh armikun **(Kërcënimet Kibernetike),** dhe vetveten **(Asetet e Informacionit),** nuk do të jetë në rrezik në 100 beteja. Ai që nuk e njeh armikunpor e njeh vetveten ndonjëherë do të fitojë dhe ndonjëherë do të humbasë. Ai që nuk e njeh as armikun dhe nuk njeh as vetveten do të jetë në rrezik në çdo betejë...“*

Sun Tzu – The Art of War

PEISAZHI KIBERNETIK - 2024

Në nivel global, "pasiguria kibernetike" mbetet një nga pesë rreziqet kryesore në Raportin Global të Rrezikut 2024 të Forumit Ekonomik Botëror

Shqipëria behet pjesë të grupit "Tier 2", që përfshin vendet që po avancojnë shpejt në fushën e sigurisë digjitale, duke treguar përkushtimin e saj për të përballuar sfidat globale të sigurisë kibernetike

Shqipëria ngjitet me 23 vende +
në Indeksin Global të Sigurisë Kibernetike (ITU)

	Pikët	Renditja	
		Botë	Europë
Raporti aktual	86.51	57	30
Raporti i mëparshëm	64.32	80	40

A është Siguria Kibernetike e njejtë me Sigurinë e Informacionit?

Siguria e Informacionit

Mbrojtja e informacionit dhe sistemeve të informacionit për të siguruar Konfidencialitetin, Integritetin dhe Disponueshëmrinë e të dhënave

Siguria Kibernetike

Aftësia për të mbrojtur përdorimin e hapësirës kibernetike nga sulmet kibernetike

PERCAKTIME TË RREZIKUT KIBERNETIK

Rreziku Kibernetik, i referohet potencialit të humbjes, dëmtimit ose dëmit në lidhje me infrastrukturën teknologjike, njerëzit dhe proceset që janë të angazhuar në menaxhimin dhe mbrojtjen e informacionit.

Rreziqet e sigurisë kibernetike lidhen me humbjen e konfidencialitetit, integritetit ose disponueshmërisë së informacionit, të dhënave ose sistemeve (ose kontrollit) të informacionit dhe reflektojnë ndikimet negative potenciale në operacionet organizative (p.sh., misioni, funksionet, imazhi ose reputacioni) asetet, individët, organizatat e tjera dhe vetë Kombin.

Mbron informacionin dhe të dhënat nga akseset e paautorizuara

Konfidencialiteti

TRIADA “CIA”

I referohet saktësisë dhe qëndrueshmërisë si dhe plotësisë dhe besueshmërisë së të dhënave.

Integriteti

I referohet aftësisë së përdoruesëve për të aksesuar informacionin kur duhet

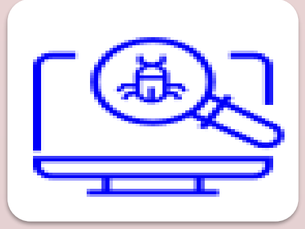
Disponueshmëria

Shembuj të rreziqeve/kërcënimeve kibernetike

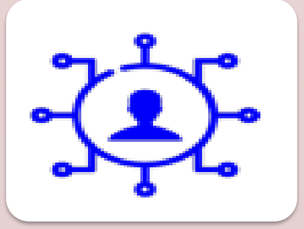
Kompromentimi i E-mail

Shkelja dhe Ekstraktimi i të dhënave

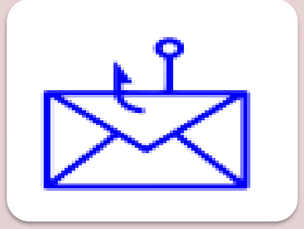
”DDoS”



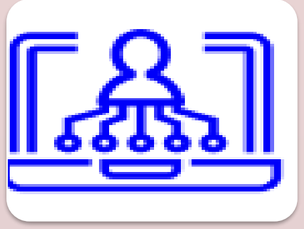
“Malware”



“Man-in-the-middle attacks”



“Phishing”

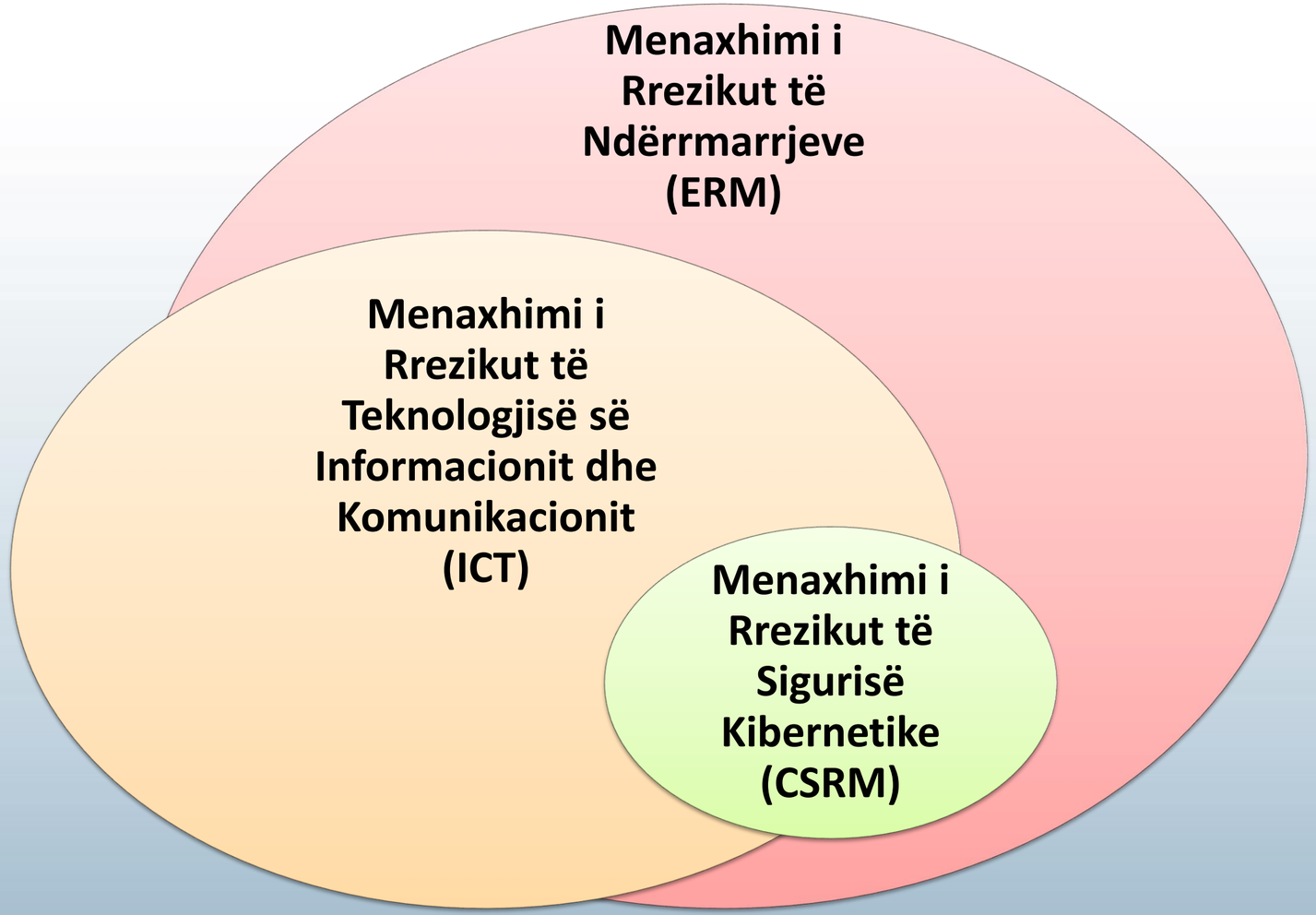


“Ransomware”

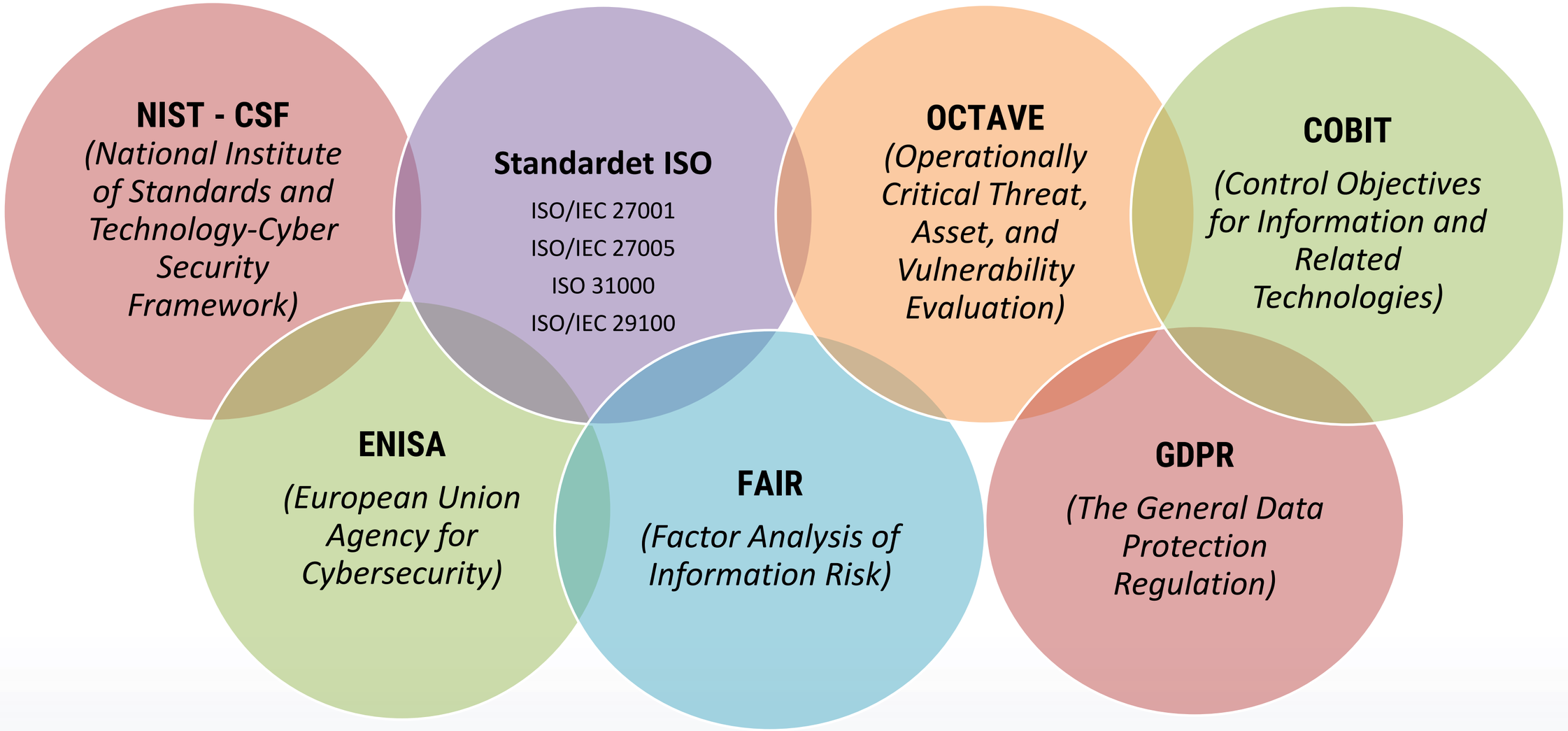
Elementët e nje kornize të menaxhimit të rrezikut kibernetik

1. Strategjia e Rrezikut Kibernetik
2. Integrimi me Kornizen e Menaxhimit te Rrezikut
3. Adoptimi i një standarti të përshtatshëm
4. Roli i Kulturës Organizative
5. Kapacitet dhe Burimet Njerëzore

2. Integrimi me Kornizen e Menaxhimit të Rrezikut



3. Kornizat Ndërkombëtare të Menaxhimit të Rrezikut Kibernetik



4. Roli i Kulturës Organizative

✓A do të prezantojë projekti i ri ndonjë rrezik të ri kibernetik?

✓A do të krijojë, heqë, amplifikojë, ose zvogëlojë ky projekt ndonjë kontroll kibernetik?

✓Ku do të ruhen të dhënat?

✓Kush duhet të ketë akses në sistemet dhe të dhënat e një projekti të ri?

✓Në çfarë mase përdoret inteligjenca artificiale në aplikacionet e reja dhe a sjell kjo ndonjë kërcënim të ri?

5. Kapacitetet dhe Burimet Njerëzore

Pavarësisht forcës së kornizës së sigurisë kibernetike të një organizate, ajo nuk do të jetë efektive pa aftësitë, ekspertizën dhe burimet njerëzore për ta zbatuar atë. Kjo përfshin tërheqjen e talentit të duhur, qoftë brenda ose jashtë organizatës, dhe trajnimin e vazhdueshëm për punonjësit në vijën e parë të mbrojtjes dhe menaxhimin.

PROCESI MENAXHIMIT TE RREZIKUT KIBERNETIK

IDENTIFIKIMI I RREZIKUT

Ku dhe çfarë lloji rreziku është i pranishëm?

VLERËSIMI I RREZIKUT

Sa i pranueshëm (serioz, impakt) është niveli aktual i rrezikut?

NDIKIMI
(Impakti)

×

MUNDËSIA E NDODHJES
(Probabiliteti)

=

VLERA E RREZIKUT

VLERËSIMI I RREZIKUT - *Koncepte*

Mundësia e Ndodhjes (Probabiliteti)

Ndikimi (Impakti/Pasoja)

Oreksi i Rrezikut

Toleranca e Rrezikut

Rreziku Rezidual (Rreziku i Mbetur)

MUNDËSIA E NDODHJES

Kategorizimi		CIA
1	Shume i Ulët	Ka një mundësi shumë të ulët që një kërcënim të materializohet dhe të ndikojë në triadën CIA.
2	I Ulët	Ka një mundësi relativisht të ulët që një kërcënim të materializohet dhe të ndikojë në triadën CIA.
3	Mesatar	Kërcënimet janë të mundshme dhe mund të ndodhin nëse nuk zbatohen masa mbrojtëse.
4	I lartë	Kërcënimet janë të mundshme dhe pritet të ndodhin nëse nuk ndërmerren masa parandaluese.
5	Shumë i Lartë	Kërcënimet janë potencialisht të sigurta që do të ndodhin dhe do të ndikojnë në triadën CIA.

NDIKIMI

Kategorizimi		CIA
1	Shume i Ulët	Zbulimi i paautorizuar i informacionit, modifikimi, prishja e tij si dhe nderprerja e aksesit/perdorimit te sistemeve/rrjeteve teknologjike te informacionit pritet te kete nje ndikim te paperfillshem per organizaten/kompanine. Efektet janë lehtësisht të menaxhueshme dhe nuk ka pritshmeri per të shkaktuar dëme ose ndërprerje te sherbimit te ofruar.
2	I Ulët	Zbulimi i paautorizuar i informacionit, modifikimi, prishja e tij si dhe nderprerja e aksesit/perdorimit te sistemeve/rrjeteve teknologjike te informacionit pritet te kete nje ndikim te ulet per organizaten/kompanine. Efektet jane te limituara dhe të menaxhueshme me burimet dhe procedurat ekzistuese per vazhdimesine e ofrimit te sherbimit.
3	Moderuar	Zbulimi i paautorizuar i informacionit, modifikimi, prishja e tij si dhe nderprerja e aksesit/perdorimit te sistemeve/rrjeteve teknologjike te informacionit pritet te kete nje ndikim te moderuar per organizaten/kompanine. Efektet në këtë kategori kanë potencialin për të shkaktuar ndërprerje të sherbimeve dhe nese nuk ndermerren masa per minimizimin ose eleminimin e tyre.
4	I lartë	Zbulimi i paautorizuar i informacionit, modifikimi, prishja e tij si dhe nderprerja e aksesit/perdorimit te sistemeve/rrjeteve teknologjike te informacionit pritet te kete nje ndikim serioz, te larte per organizaten/kompanine. Efektet jane te konsiderueshme dhe mund të shkaktojne ndërprerje te rendesishme te sherbimit nëse nuk trajtohen brenda nje kohe te shkurter dhe nuk merren masat e duhura ne ruajtjen e vazhdimesise se sherbimit te ofruar.
5	Shumë e Lartë/ Kritik	Zbulimi i paautorizuar i informacionit, modifikimi, prishja e tij si dhe nderprerja e aksesit/perdorimit te sistemeve/rrjeteve teknologjike te informacionit pritet te kete nje ndikim jashtezakonisht te rende, kritik per organizaten/kompanine. Efektet e ndikimit jane ne nivelin më të lartë dhe kërkojnë vëmendje të menjëhershme. Ekziston potenciali shume i larte për dëme serioze, te pariparueshme duke rrezikuar vazhdimesine e punes dhe ofrimin e sherbimit pertej kohes se toleruar.

VLERËSIMI I RREZIKUT - Matrica

*Rreziku = Mundësia e Ndodhjes * Ndikim*

MUNDËSIA		NDIKIMI				
		Shumë i ulët (1)	**I Ulët (2)**	**Mesatar (3)**	**I lartë (4)**	**Shumë i lartë (5)**
	Shumë i ulët (1)	1	2	3	4	5
	I Ulët (2)	2	4	6	8	10
	Mesatar (3)	3	6	9	12	15
	I lartë (4)	4	8	12	16	20
	Shumë i lartë (5)	5	10	15	20	25

TRAJTIMI I RREZIKUT ME OREKSIN E RREZIKUT

Vlera e Rrezikut	Niveli i rrezikut	Koha e Trajtimit
[1-3]	Shumë i ulët	Nuk ka nevoje për trajtim
[4-6]	E ulët	Nuk ka nevoje për trajtim
[7-11]	Mesatar	Ka nevojë për trajtim brenda afatit kohor prej 12 muajsh
[12-19]	I Lartë	Ka nevojë për trajtim brenda afatit kohor prej 6 muajsh
[20-25]	Shume i lartë	Ka nevojë për trajtim brenda afatit kohor prej 3 muajsh

MITIGIMI (ZBUTJA) E RREZIKUT

- Masat Parandaluese
- Monitorim i Vazhdueshëm
- Planifikimi i Reagimit ndaj Incidenteve
- Edukim dhe Ndërgjegjësim

MONITORIMI DHE RISHIKIMI

Siguria kibernetike kërkon përpjekje të vazhdueshme. Infrastruktura duhet të angazhohet në monitorim të vazhdueshëm dhe të kryejë rishikime periodike për t'u adapatuar ndaj kërcënimeve të reja dhe ndryshimeve në mjediset e biznesit. Kjo ndihmon në sigurimin që strategjitë e menaxhimit të rrezikut të mbeten efektive dhe relevante.

Skenarë/Raste Praktike mbi Menaxhimin e Rrezikut Kibernetik

Skenari 1: Phishing në një Kompani Konsulente

****Situata**:** Je punonjës në një kompani konsulence. Marr një email nga shefi që kërkon me urgjencë një dokument të ndjeshëm për klientin, me një lidhje për ta ngarkuar dokumentin.

****Çfarë bën?****

Opsioni A: Klikon mbi lidhjen dhe ngarkon dokumentin sa më shpejt.

Opsioni B: Kontrollon adresën e emailit dhe diskuton me përgjegjësin/eprorin për të konfirmuar kërkesën.

Opsioni C: Fshin e-maili dhe nuk bën asgjë.

****Zgjidhja më e mirë**: OPSIONI B**

Skenari 2: Ransomware në Institucionin Arsimor

****Situata**:** Punon në departamentin e IT-së të një universiteti dhe zbulon që disa dosje/file të rëndësishme janë bllokuar, duke shfaqur një mesazh kërkese për para në shkëmbim të aksesit.

****Çfarë bën?****

Opsioni A: Paguan shumën për të rikthyer askesin, pasi të dhënat janë shumë të rëndësishme.

Opsioni B: Izolon sistemin nga rrjeti, informon ekipin e sigurisë dhe përdor kopje rezervë për të rikuperuar të dhënat.

Opsioni C: Injoron problemin dhe vazhdon me punën, duke shpresuar që të zgjidhet vetë.

****Zgjidhja më e mirë**: OPSIONI B**

Skenarë/Raste Praktike mbi Menaxhimin e Rrezikut Kibernetik

Institucioni i Shëndetësisë – Menaxhimi i të Dhënave të Pacientëve

****Sfidat**:** Spitali kishte të dhëna të ndjeshme të pacientëve dhe duhej të siguronte që stafi të përdorte vetëm informacionin e nevojshëm për detyrat e tyre. Shumë anëtarë të stafit, pa qenë nevoja, kishin akses në të dhënat e pacientëve, duke krijuar rreziqe për privatësinë e tyre.

****Zgjidhja**:** Institucioni zbatoi një sistem kontrolli për të kufizuar aksesin vetëm për ata që kishin një rol specifik.

****Rezultatet**:** Shkeljet e privatësisë u reduktuan ndjeshëm, dhe pacientët ndiheshin më të sigurt që informacionet e tyre ishin të mbrojtura

Kompania e Marketingut – Sigurimi i Fjalëkalimeve dhe Përdorimi i MFA

****Sfidat**:** **: Një anëtar i stafit kishte përdorur një fjalëkalim të dobët dhe të njëjtin në disa llogari, gjë që e bëri të lehtë për hakerat të futeshin në llogarinë e tij dhe të ndikonin të dhënat e klientëve

****Zgjidhja**:** Kompania vendosi rregulla për fjalëkalimet dhe zbatimin e vërtetimit/autentifikimit me dy faktorë (MFA) për çdo llogari të rëndësishme.

****Rezultatet**:** Reduktimi i shkeljeve për shkak të fjalëkalimeve, duke rritur sigurinë dhe besueshmërinë e klientëve të tyre.

AUTORITETI KOMBËTAR I SIGURISË KIBERNETIKE
aksk.gov.al

https://aksk.gov.al

AKSK | Legjislacioni | Shërbime Të Besuara | Evente | Publikime | Njoftime | Programi I Transparencës | Kontakt | Raporto

Vajzat Dhe Gratë Në Sigurinë Kibernetike: Workshop I Organizuara Nga AKSK Me Mbështetjen E OSCE Në Shqipëri

Më shumë

Shqipëria Ngjitet Me 23 Vende Në Indeksin Global Të Sigurisë Kibernetike 2024, Sipas ITU

Më shumë

Zhvillohet Konferenca Kombëtare E Sigurisë Kibernetike – AKSK Prezanton Arritjet E Shqipërisë Në Fushën E Sigurisë Kibernetike

Më shumë

Testo Institucionin

Faleminderit!