7. GESTIONAREA RISCULUI CIBERNETIC

Preliminarii

În această temă vor fi explorate în profunzime conceptul de vulnerabilitate al activelor informaționale și relevanța managementului riscului cibernetic în protejarea resurselor critice. Vor fi analizate diferite tipuri de vulnerabilități, metode de evaluare a riscului și strategii de gestionare a riscurilor cibernetice, oferind o perspectivă cuprinzătoare asupra modului în care organizațiile pot gestiona problemele legate de securitatea cibernetică.

Scopul:

- *studierea metodelor de evaluare și minimizare a riscului cibernetic, calcularea valorii calitative și cantitative a riscului asociat activelor informaționale.*

Obiectivele educaționale:

- *cunoașterea metodelor de evaluare a vulnerabilităților activelor informaționale;*
- *studierea metodelor de management al riscului cibernetic;*
- *calcularea riscului cibernetic privind activele informaționale importante.*

Finalitățile de referință:

- *capacitatea de a evalua vulnerabilitățile activelor informaționale;*
- *cunoașterea metodelor de gestionare ale riscului cibernetic;*
- *familiarizarea cu metodele cantitative și calitative de evaluare a riscului cibernetic;*
- *dezvoltarea abilităților de realizare în cadrul unei companii specifice a procesului de gestiune a riscului cibernetic.*

Modalitățile de evaluare

Evaluarea masteranzilor se va efectua în baza testelor formative realizate pe parcursul semestrului de studiu, care vor conține întrebări de tip grilă, întrebări deschise și studii de caz. De asemenea, masteranzii vor îndeplini sarcini practice individuale sau de grup și vor prezenta oral o temă relevantă domeniului de securitate cibernetică. La finele semestrului masteranzii vor susține un examen care va acoperi toate temele din acest suport de curs.

7.1. Evaluarea vulnerabilităților

În era informațională actuală, informația a devenit unul dintre cele mai prețioase active pentru organizații de toate dimensiunile și din toate sectoarele economiei mondiale. De la datele financiare și planurile strategice la informațiile personale ale clienților și secretele comerciale, protecția activelor informaționale este esențială pentru succesul și continuitatea unei afaceri. Cu toate acestea, complexitatea și interconectivitatea sistemelor informaționale moderne le fac vulnerabile la o gamă largă de amenințări cibernetice.

Vulnerabilitățile activelor informaționale pot lua multe forme, inclusiv deficiențe în securitatea software-ului, erori umane, acces neautorizat și atacuri cibernetice sofisticate. Aceste vulnerabilități pot fi exploatate de atacatori pentru a compromite confidențialitatea, integritatea și disponibilitatea informațiilor, cauzând pierderi financiare semnificative, daune reputaționale și implicații legale pentru organizații.

În acest context, managementul riscului cibernetic devine un aspect critic al guvernanței corporative. Managementul riscului cibernetic implică identificarea, evaluarea și prioritizarea riscurilor asociate cu activele informaționale, precum și implementarea de măsuri de control adecvate pentru a minimiza aceste riscuri. Printr-o abordare sistematică și proactivă,

organizațiile pot dezvolta strategii de apărare eficiente, pot răspunde rapid și eficient la incidentele de securitate și pot asigura reziliența infrastructurilor lor informaționale.

Vulnerabilitățile cu impact major sunt cele pe care le prezintă activele informaționale: hardware, software, rețea și comunicații sau informația.

Metodologia de evaluare a vulnerabilităților include:

1. ***Inventarierea sistemelor, a activelor informaționale și de rețea*** **–** fără a avea lista activelor informaționale ale organizației nu se pot cunoaște vulnerabilitățile sistemului gestionat, pentru aceasta pot fi utilizate software-uri dedicate.
2. ***Documentarea și testarea vulnerabilităților depistate*** **–** pentru documentare pot fi utilizate bazele de date așa ca CVE list, care conține toate vulnerabilitățile cunoscute.
3. ***Evaluarea vulnerabilităților***, a procesului de eradicare a acestora sau de acceptare a vulnerabilității, în dependență de decizia pe care o ia organizația, include:
   - selectarea instrumentelor;
   - dezvoltarea procedurilor;
   - formalizarea metodologiei;
   - training-uri pentru personal;
   - evaluarea propriu-zisă a vulnerabilității.
4. ***Comunicarea informației despre vulnerabilitățile identificate*** proprietarilor activelor informaționale vulnerabile.
5. ***Evaluarea riscului de securitate și raportarea*** acestuia managementului superior.
6. ***Implicarea managementului superior*** pentru identificarea strategiilor abordate față de vulnerabilitățile nerezolvate.

Pentru evaluarea vulnerabilităților (figura 8.1) este necesar a evalua vulnerabilitățile pe care le prezintă [8]:

- internet-ul;
- intranet-ul;
- platformele și software-ul cu care lucrează compania;
- Rrțelele fără fir.

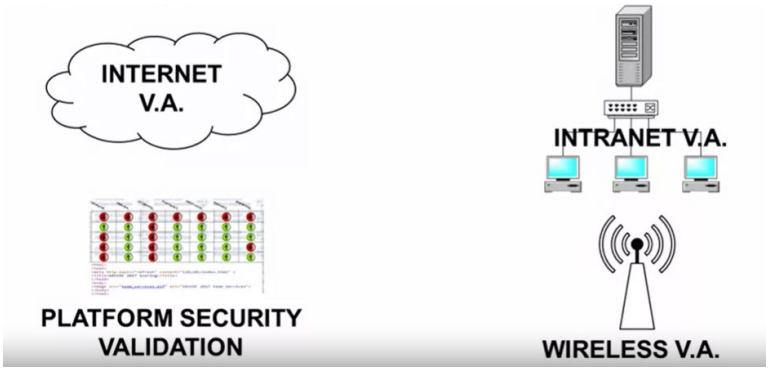

Fig. 8.1. Ceea ce trebuie evaluat [8]

Evaluarea vulnerabilităților poate avea loc lunar, trimestrial sau anual, în dependență de activitatea comercială desfășurată. Cu cât mai mare este durata dintre evaluări, cu atât mai mare este riscul că o anumită vulnerabilitate neidentificată la timp va fi exploatată de către un atacator. Evaluarea vulnerabilităților poate fi externalizată prin angajarea unei companii specializate sau pot fi realizate teste de penetrare pentru identificarea vulnerabilităților. Testele de penetrare diferă mult de evaluarea vulnerabilităților. În evaluarea vulnerabilităților au loc analize care nu intervin nicicum în buna funcționare a sistemului, pe când un pen-tester va acționa ca și un atacator pentru a identifica vulnerabilitățile din sistem, după care pregătește un raport care este prezentat managementului superior. Acest fapt și îl face diferit de un atacator.

Testele de penetrare sunt executate utilizând:

- Cutia neagră (black-box) – în cazul când testerul nu cunoaște nimic despre sistemele organizației (figura 8.2).

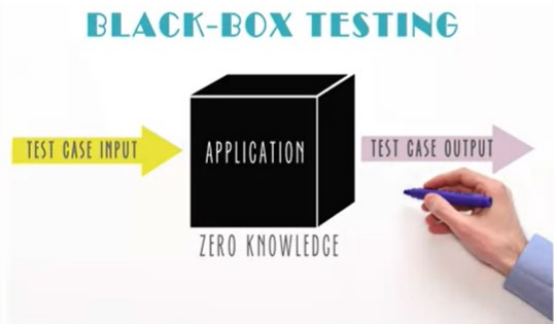

Fig. 8.2. Black-Box [3]

- Cutia albă (white box) – când pen-testerul este informat despre configurațiile sistemului, este realizat când există anumite suspiciuni în privința personalului organizației (figura 8.3).

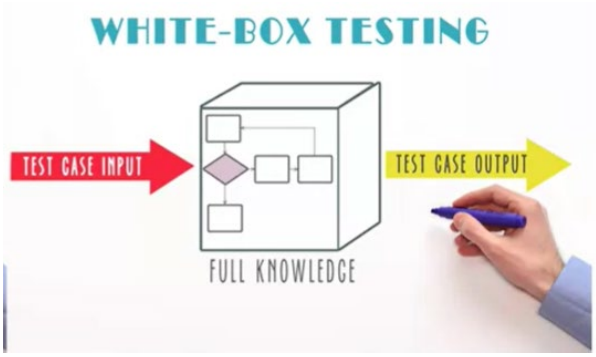

Fig. 8.3. White-box [3]

Instrumente și tehnici

Pentru identificarea vulnerabilităților din sistem atacatorii efectuează următorii pașii

- Colectarea informațiilor despre companie, angajați, activitate etc., utilizând motoarele de căutare, tehnici de inginerie socială.
- Analiza codului sursă a site-ului companiei pentru a identifica și alte informații despre companie.
- Utilizarea comenzilor prin care se pot identifica adresele IP publice ale companiei.
- Scanarea adreselor de rețea și identificarea porturilor logice deschise, a protocoalelor de rețea utilizate de companie; un astfel de instrument este NMAP [25], astfel încât auditul porturilor deschise și închiderea porturilor care nu sunt necesare companiei va reduce riscul atacului.
- Identificarea sistemelor de operare utilizate de companie este un pas important, pentru aceasta se folosesc scanere de vulnerabilitate așa ca OpenVas.
- Utilizarea exploit-urilor de vulnerabilități cum ar fi Metasploit.
- Utilizarea snifferelor de pachete ca Wireshark pentru a captura tot traficul din rețea [25].

Strategii de remediere a vulnerabilităților:

- Apărare – organizația implementează anumite controale de securitate pentru a eradica vulnerabilitatea, deoarece este vorba despre active importante pentru organizație.

- Atenuare – organizația înțelege că acest activ ar putea fi atacat și implementează planul de răspuns la incidente, pentru ca în cazul când un atac va avea loc să se cunoască ce trebuie făcut, sau planul de recuperare în caz de dezastre, planul de continuitate al afacerii sau planul de criză.
- Transfer – vulnerabilitatea este transferată către o altă organizație care va fi responsabilă de managementul acesteia, outsourcing, sau către o companie de asigurări care va plăti compensații în cazul pierderii activului.
- Acceptare – în cazul activelor cu valoare mică în companie, organizația decide să accepte această vulnerabilitate, deoarece activul nu reprezintă valoare importantă în procesele de afaceri. O altă cauză este costul controlului de securitate, care poate fi mai mare decât valoarea activului.
- Terminare – în cazul activelor care pot fi pur și simplu scoase din uz, nefiind necesare companiei.

Alegerea strategiei de remediere a vulnerabilităților depinde de valoarea activului. Pentru activele valoroase de obicei se utilizează apărarea, atenuarea și transferul, iar pentru cele cu valoare mică sau mai puțin importante se utilizează acceptarea sau terminarea.

Remedierea vulnerabilităților este un proces foarte scump, de aceea se efectuează managementul riscului și se calculează costul beneficiului, pentru a evalua cât va costa remedierea vulnerabilităților identificate în sistem.

7.2. Managementul riscului cibernetic

Managementul riscului include activități coordonate pentru a dirija și a controla o organizație în ceea ce privește riscul. Riscul cibernetic poate fi definit ca *un eveniment de securitate care a exploatat o vulnerabilitate în sistemul informațional și a cauzat amenințarea*. Evenimentul de securitate al informațiilor reprezintă apariția identificată a unei stări de sistem, serviciu sau rețea care indică o posibilă încălcare a politicii de securitate a informațiilor, sau eșecul controalelor, ori o situație necunoscută anterior care poate fi relevantă pentru securitate și are asociate o consecință și o probabilitate. La baza analizei riscului cibernetic stă procesul de identificare a amenințărilor. Amenințările sunt definite ca „*orice fenomen (proces, eveniment) nedorit din punct de vedere al funcționării neperturbate a unui sistem*” [9].

Scopul acestei etape este de a evalua riscul cibernetic al activelor informaționale. Abordarea holistică a managementului securității este esențială, deoarece permite o perspectivă de ansamblu asupra tuturor resurselor care necesită a fi protejate. Metodele de evaluare a riscului trebuie să ia în considerație dependențele dintre resursele ce asistă serviciile electronice. Astfel, metodele trebuie să aibă capacitatea de a se adapta, să fie dinamice și potrivite pentru organizație. Deoarece serviciile electronice sunt în continuă modificare, factorii de risc se modifică și afectează activitatea organizației, iar managementul riscului este tot mai important.

Standardul ISO 31000 definește cadrul standardizat după care poate fi realizat managementul riscului în organizații la care se conformează și standardul ISO 27005. În figura 8.4 este reflectat procesul de management al riscului.

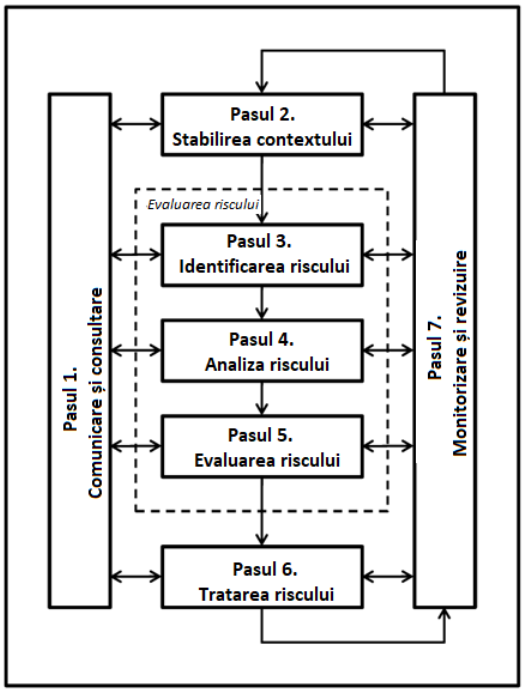

Fig. 8.4. Procesul de management al riscului [9]

Procesul reprezentat în figura 8.4 trebuie să fie obligatoriu iterativ și să se repete la anumite perioade specificate sau când au loc modificări în sistemele informaționale ale organizațiilor.

Standardul ISO 27005 abordează riscurile de securitate prin perspectiva activelor informaționale definite ca orice bun ce are valoare pentru organizație și necesită protecție. Conform standardului ISO 27005, toate activele informaționale trebuie să fie clasificate în *active primare* și *active de suport*.

Activele primare sunt procesele de afaceri ale organizațiilor, ca de exemplu: vânzări, prestare servicii, educație și desigur informația. Informația urmează a fi clasificată conform standardului în *confidențială, restricționată* și *publică*.

Activele de suport necesită inițial, conform standardului ISO 27005, să fie clasificate conform categoriilor din care fac parte. Tabelul 8.1 inserează categoria și activele de suport corespunzătoare.

Tabelul 8.1. Cartografierea activelor de suport

1	*2*	*3*	*4*
Nr.	***Categorie***	***Activ de suport***	***Exemple***
1	**Echipamente (componente hardware)**	Echipamente non-portabile	○ Stații de lucru fixe ○ Servere
		Echipament portabil	○ Laptop ○ Tablete ○ Smartphone
		Periferice de procesare	○ Imprimante ○ Harddiscuri externe ○ Scanere
		Medii electronice	○ Medii amovibile ○ CD-ROM
		Alte medii	○ Hârtie ○ Fax
2	**Software**	Sisteme de operare	○ Server: Linux, Windows Server

1	*2*	*3*	*4*
			○ Stații de lucru: Linux, Windows Server
		Servicii, mentenanța sau administrarea software	Nu sunt direct accesibile utilizatorilor, dar susțin funcționarea conformă a SO
		Pachete software sau software standard	○ Software pentru bazele de date ○ Software pentru serverele web ○ Software Active Directory
		Aplicații de afaceri	- ***Standard:*** ○ Software pentru controlul accesului ○ Software administrativ - ***Specifice:*** ○ Medii în care s-a dezvoltat diferit software specializat pentru afaceri
3	**Rețea și comunicații**	Medii și suporturi	○ Protocoale Wireless WiFi 802.11 ○ Ethernet ○ Bluetooth ○ FireWare ○ ADSL
		Echipament de rețea	○ Switch ○ Router
		Interfețe	○ Adaptor Ethernet ○ Fibră optică ○ Antene radio
4	**Personal**	Factorii de decizie (top managementul organizației)	○ CEO ○ CFO, CIO, COO ○ CISO etc.
		Utilizatorii cu acces special	○ Angajații de la resurse umane ○ Managerii financiari ○ Contabilitatea
		Personal de operare / mentenanță	○ Administrator de sistem ○ Operator date, back-up ○ Inginerii ○ Ofițerii de securitate
		Dezvoltatorii	○ Dezvoltatorii bazelor de date ○ Dezvoltatorii de diferite aplicații de afaceri
5	**Infrastructura**	Mediul extern	○ Domiciliul angajaților din care se conectează la rețeaua organizației
		Premise	○ Organizația ○ Clădirile ○ Mijloacele de supraveghere video din exterior
		Zone formate	○ Birouri ○ Săli de conferințe ○ Zone industriale și de producție ○ Camera serverelor
		Servicii esențiale	○ Ce susțin buna funcționare a organizației
		Comunicații	○ Internet ○ VOIP ○ Rețele telefonice interne

1	*2*	*3*	*4*
		Utilități	○ Furnizarea de energie echipamentului și perifericelor de IT (UPS, generatoare) ○ Alimentare cu apă ○ Eliminarea deșeurilor ○ Aer condiționat
6	**Structura organizației**	Autorități	○ Ministerele de resort
		Structura organizației	○ Serviciul achiziții ○ Serviciul resurse umane ○ Serviciul social ○ Departamentul de IT etc.
		Proiect sau sistem organizațional	○ Dezvoltarea și implementarea în întreprindere a aplicațiilor noi
		Subcontractori/ producători	○ Organizații ce prestează anumite servicii pentru organizații

Conform standardului de securitate ISO 27005, activele de suport pot asista unul sau mai multe active primare, procese de afaceri, de aceea este foarte important a crea dependențe; analiza va avea un rezultat mult mai precis și corect estimat [26], deoarece procesele de afaceri sunt sursele primare de securitate. Pentru evaluarea riscului cibernetic se iau în considerație impactul și probabilitatea ca un anumit incident de securitate să aibă loc.

O sursă importantă pentru evaluarea impactului reprezintă interviurile cu proprietarii proceselor secundare, cu administratorii de rețea și alte persoane interesate [27]. Criteriile după care poate fi evaluat impactul riscului cibernetic sunt reflectate în tabelul 8.2.

Tabelul 8.2. Criteriile de evaluare a impactului

1	*2*	*3*
Valoarea calitativă	***Valoarea numerică***	***Descrierea impactului***
Neglijabil	1	Nu implică costuri suplimentare, serviciile nu sunt întrerupte, reputația organizației nu este afectată, încălcare neesențială a obiectivelor de securitate.
Redus	2	Implică costuri reduse, indisponibilitatea serviciilor de scurtă durată, mici pierderi ale datelor și impact minor asupra confidențialității.
Mediu	3	Implică costuri medii, indisponibilitatea serviciilor pe o anumită perioadă de timp, pierderi ale datelor și impact mediu asupra reputației, impact mediu asupra confidențialității datelor electronice.
Sporit	4	Implică costuri înalte, are ca efect indisponibilitatea de lungă durată a serviciilor, pierderea datelor electronice sau încălcarea integrității datelor importante, așa ca datele personale, proprietatea intelectuală, secretul comercial. Efect negativ accentuat asupra reputației organizației.

Probabilitatea poate fi exprimată prin frecvența cu care amenințările încearcă să exploateze vulnerabilitățile sistemului. În tabelul 8.3 sunt incluse criteriile de evaluare a probabilității.

Tabelul 8.3. Criterii de evaluare a probabilității [27]

Valoarea calitativă	*Valoarea numerică*	*Descrierea probabilității*
Neglijabilă	1	Incidentul de securitate are loc o dată pe an
Redusă	2	Incidentul de securitate are loc o dată în trimestru
Medie	3	Incidentul de securitate are loc o dată în lună
Sporită	4	Incidentul de securitate are loc săptămânal

Formula aplicată pentru a calcula valoarea riscului cibernetic este:

$$R=Probabilitatea * Impactul \quad (8.1)$$

Criteriile de evaluare a riscurilor cibernetice sunt următoarele:
- *risc redus*: de la 1-4 (riscul este acceptat);
- *risc mediu*: de la 5-9 (riscul este acceptat condiționat);
- *risc sporit*: de la 10-16 (riscul nu poate fi acceptat).

Criteriile de evaluare a riscurilor cibernetice sunt analizate din perspectiva impactului avut asupra celor 3 obiective de securitate: confidențialitatea, integritatea și disponibilitatea.

Tabelul 8.4. Valoarea riscului cibernetic

Probabilitatea / ***Impactul asupra organizației***	***1***	***2***	***3***	***4***
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

După rezultatele identificate în tabelul 8.4 se poate observa că pentru un impact foarte înalt, dacă probabilitatea ca acest incident va avea loc este neglijabilă, înseamnă că și riscul rezultat va avea o valoare joasă. Astfel se verifică valoarea riscului cibernetic și se iau decizii administrative în funcție de criteriile de evaluare a riscurilor specificate mai sus.

Pentru analiza riscului se recomandă identificarea activelor și valorificarea lor prin prisma relațiilor dependente ce există între activele de suport [27]. De asemenea este foarte important a calcula costul activului și costul riscului existent, fiindcă nu se implementează cerințe de securitate ce costă mai mult decât valoarea activului protejat, rentabilitatea economică având un rol important când are loc evaluarea riscului.

Conform ISO 27005, fiecărui activ informațional i se atribuie câte un proprietar, care nu va deține de drept acest bun, însă va fi responsabil și va contabiliza activul și tot această persoană va fi proprietarul riscului asociat activului.

Tabelul 8.5. Identificarea proprietarilor activelor informaționale

Nr.	*Activul primar*	*Categoria activului*	*Adresa*	*Proprietarul activului*
1	Proces de afaceri 1	Primar	Str.....	Domnul/doamna X/ Departamentul X
2	Proces de afaceri 2	Primar	Str...	Domnul/doamna Y /Departamentul Y
3	Proces de afaceri 3	Primar	Str...	Domnul/doamna Z / Departamentul Z
4	Router de bază	Suport	Str...	....

Se recomandă a utiliza baze de date de management al configurației (BDMC), care servesc drept sursă importantă pentru managementul activelor informaționale, deoarece oferă detalii importante și permit a adăuga, șterge sau modifica activele informaționale. Deși BDMC nu este responsabil direct de colectarea datelor/activelor, oferă totuși contextul și depozitul necesar pentru a gestiona activele informaționale.

După identificarea activelor informaționale este necesar a determina valoarea acestora pentru organizație. Standardul ISO 27005 admite atât evaluarea calitativă, cât și evaluarea cantitativă, fiind o metodă hibridă de management al riscurilor de securitate. Pentru evaluarea calitativă a activului pot fi utilizate următoarele calificative: neglijabil, scăzut, mediu, înalt și foarte înalt. Cel mai frecvent se implementează trei calificative: scăzut, mediu, înalt. Aceasta depinde de dimensiunea organizației și de diversitatea serviciilor electronice pe care le prestează. Sub-procesele recomandate sunt: identificarea activului, atribuirea activului de suport către procesul de afaceri, calcularea valorii calitative independente a activului după costul și impactul avut în procesul de afaceri aferent, determinarea valorii dependente a activului și ultimul pas este identificarea valorii totale a activului informațional. Astfel, valoarea totală a activului dependent reprezintă suma valorii independente și maximum valorii activelor de care acesta depinde, relație reprezentată în formula 8.2:

$$V_t = V_{ind} + V_{dep}, \tag{8.2}$$

unde:

V_{ind} – poate fi calculată ca suma dintre costul activului și impactul estimat al activului de suport în procesul de afaceri;

V_{dep} – suma importanței maxime a activelor de care depinde securitatea activului specificat.

Astfel, urmează să fie calculată mai întâi valoarea independentă a activelor, care depinde de costul activului și de impactul pe care îl are în procesele secundare. În tabelele 8.6 și 8.7 se poate observa conversia în valori calitative a costului activului informațional și impactul avut de activ în procesul de afaceri.

Tabelul 8.6. Conversia costului activului într-o valoare calitativă [27]

Valoarea calitativă		***Descrierea***
nivel	***scară***	
Redus	1	Valoarea activului pentru reparație sau înlocuire e mai mică decât 5000 lei
Mediu	2	Valoarea activului pentru reparație sau înlocuire este în intervalul 5000-15000 lei
Sporit	3	Valoarea activului pentru reparație sau înlocuire este mai mare decât 15000 lei

Tabelul 8.7. Conversia impactului activului în procesul academic [27]

Valoarea calitativă		***Descrierea***
nivel	***scară***	
Redus	1	Activul informațional nu are impact asupra proceselor de afaceri
Mediu	2	Reprezintă activ de suport pentru procesul de afaceri
Sporit	3	Activul informațional este important și are impact critic asupra procesului de afaceri

Un ultim aspect care susține managementul eficient al riscului cibernetic este instruirea periodică a utilizatorilor sistemelor informaționale atât în momentul angajării (valabil pentru personal), cât și la intervale definite de timp, cu o periodicitate cel puțin anuală. Instruirea

periodică ar trebui să includă informații despre atacurile cibernetice ce vizează compania, cu precădere cele care vizează factorul uman, așa cum sunt atacurile de inginerie socială. Ar trebui să fie clar descrise semnăturile atacurilor, care îi vor ajuta pe utilizatorii finali să identifice tentativele specifice diferitor tipuri de amenințări de securitate, deoarece orice acțiuni de reducere a riscului cibernetic din partea specialiștilor pot eșua în cazul în care utilizatorii finali nu respectă cerințele de securitate în utilizarea sistemelor informaționale.

Întrebări și subiecte pentru aprofundarea cunoștințelor

1. Cum poate fi explicată vulnerabilitatea diferitor tipuri de active informaționale? Dați cel puțin câte 3 exemple relevante pentru fiecare clasă de active.
2. Care este importanța activelor informaționale în realizarea proceselor de afaceri ale unei companii?
3. Care sunt pașii necesari pentru managementul riscului cibernetic?
4. Cum se poate calcula valoarea activelor informaționale dependente?
5. Explicați necesitatea realizării managementului riscului. Care sunt etapele de realizare ale acestui proces?
6. Cum se reflectă instruirea personalului asupra procesului de asigurare al securității cibernetice?
7. De ce este necesar ca activele informaționale să aibă atribuit un proprietar?
8. Ce este managementul riscului? De ce este atât de importantă identificarea riscurilor și vulnerabilităților activelor informaționale în managementul riscurilor?
9. În strategiile de management al riscului, de ce trebuie să facă parte din proces revizuirea periodică a riscului?
10. Ce sunt vulnerabilitățile? Cum are loc identificarea vulnerabilităților?