ფინალური იუმ

დავალებები - 10 ქ

რა არის ISO? რა არის ISO 27001 სტანდარტი? როგორ უზრუნველყოფს ორგანიზაცია ამ სტანდარტს?

ISO არის ორგანიზაცია რომელიც აწესებს მსოფლიო სტანდარტებს ხარისხის გაუმჯობესის მიზნის.

ISO 27001 არის ინფორმაციული უსაფრთოების მართვის სისტემების(ISMS) სტანდარტი. სტანდარტი საშუალებას აძლევს კომპანიას ან ორგანიზაციას დაამყაროს, დანერგოს, შეინარჩუნოს და მუდმივად გააუმჯობესოს თავიანთი ინფორმაციული უსაფრთხოების პროცესები. 27001 სტანდარტთან შესაბამისობა უნდა ვუზრუნველყოთ კონტროლის მექანიზმებით მათ შორის რისკების მართვა უნდა იყოს თანხვედრაში ჩვენს ორგანიზაციაში დანრეგილი კონტროლის მექანიზმებთან.

სტანდარტის ძირიტადი მიმართულებებია:

- **ბიზნეს პროცესების აღწერა და აქტივების შეფასებას** ,
- **რისკების მოდული**
  - მოიცავს აქტივებიდან გამომდინარე რისკების შეფასებას, საფრთხეების მისადაგებას და მის აღწერას
- **კონტროლის მექნანიზმები**
  - საპირისპირო ქმედება რომლითაც რისკს ვამცირებთ და უსაფრთხოს ვქმნით გარმოს
  - ჩვენ ვახდენთ საოპერაციო და ორგანიზაციული გარემოს უსაფრთხოებას.
- **ამ ყველაფრის მონიტორინგი**
  - უნდა თვალყური ვადევნოთ რამდენად თანხვედრაშია რისკები
- **აუდიტი** - პირველი მეორე და მესამე მხარეის აუდიტები
  - პირველი - შიდა აუდიტი, როდესაც ჩვენ ვამოწმებთ ჩვენსავე სისტემას
  - მეორე -გარე აუდიტი, ჩვენ გვამოწმებს დამკვეთი ან ვამოწმებთ მომწოდებელს
  - მესამე - როდესაც გვამოწმებს დამოუკიდებელი სერტიფიცირების ორგანო

რა არის კონტროლის მექანიზმები და როგორია კონტროლის მექანიზმები კლასიფიკაცია?

კონტროლის მექანიზმი არის პოლიტიკა, პროცედურა, სტრატეგია ან ინსტრუმენტი რომელიც ამცირებს რისკის დონეს. არსებობს შემდეგი კონტროლის მექანიზმის ტიპები:

- **პრევენციული** - არასასურველი მოვლენის თავიდან აცილება სანამ ის მოხდება
  - საკეტები
  - ღობე

    - dummy cameras(ვიდეო კამერა რომელიც არ მუშაობს)
    - ვაქცინაცია
    - შიფრაცია
- **დეტექციური** - ახდენს მოვლენის აღმოჩენას(დეტექციას), არსებული პრობლემის გამოვლენას
    - ვიდეკომარა
    - ლოგირება
    - ანტივირუსული პროგრამები
    - სკანირება
- **შემაკავებელი** - მიზნად ისახავს არასასურველი ქცევის ან მოვლენის წარმოშობის თავიდან აცილებას ან მათ შეზღუდვას
    - ვიდეოკონტროლის გამაფრთხილებელი ნიშანი
    - USB პორტების დაბლოკვა
    - თანხის მაქსიმალური ლიმიტის დაწესება
- **მაკორექტირებელი** - არასასურველი მოვლენის შემდეგ ავტომატურად აქტიურდება, როდესაც მოვლენა უკვე გამოვლენილია პრობლემა და საჭიროა ზიანის მინიმუმამდე დაყვანა
    - არასანქცირებულ წვდომის აღმოჩენის დროს პაროლის ცვლილება
    - ვირუსის აღმოჩენის ჩემდეგ დაზიანებული ფაილის აღდგენა
    - არასწორი ტრანზაქციის შემდეგ თანხის ანულირება
- **მაკომპენსირებელი -** გამოიყენება მაინ როდესაც სხვა ტიპის კონტროლის მექანიზმები ვერ ხორციელდება ეფექტურდ
- **აღდგენითი -** გამოიყენება ზიანის მიღების შემდეგ სისტემის აღსადგენად და მის პირვანდელ მდგომარეობაში დასაბრუნებლად
    - სარეზერვო ასლები (backup)

რა კონტორლის მექანიზმების ტიპები არსებობს?

- **ფიზიკური** - მატერიუალური სახით არსებული კონტოლები
    - საკეტები
    - ღობეები
    - დაცვის თანამშრომელი
- **ტექნიკური** - ინფორმაციული სისტემები ან ინფორმაციული სისტემის კომპონენტები
    - აუდიტის ჩანაწერები (ლოგები)
    - კომპიუტერზე წვდომის კონტროლები
    - Firewall
- **ადმინისტრაციული** - კონტროლები რომლითაც ხდება მართვა
    - პოლიტიკები
    - პროცედურები
    - პროტოკოლები
    - კონფიგურაციები

მოცემული იქნება ალბათ ატქივი და ჩვენ უნდა შევუსაბამოთ საფრთხეები და კონტროლის მექანიზმები მაგალითად (არ არის საჭირო ენციკლოპედიური ენით დავწეროთ, გასაგები იყოს მთავარია):
სამუშაო ლეპტოპი და მისი საფრთხე არის მაგალითად მოპარვა,

პრევენციისთვის კი შეიძლება გამოყენებულ იქნას სამაგრები რომელითაც მომაგრებული ქინება რაიმეზე.

ღია კითხვები

- **რას გულისხმობს ინფორმაციული აქტივი კონცეპტუალურ დონეზე, მოიყვანეთ მაგალითი**
  - ყველა ღირებული რესურსი რომელიც დაკავღიებულია ინფრომაციასთან მის დამუშავება, შენახვა, გადაცემა ან დაცვასთან შეიძლება ჩაითვალოს ინფორმაციულ აქტივად. მაგალითად ორგანიზაციაში წარმოებული რაიმე ჩანაწერი როგორიცაა მომხმარებელის ინფორმაცია ფინანსური ჩანაწერები, IT ინფრასტრუქურა მონაცემთა ბაზები ან სხვა. ინფორმაციული აქტივი შეიძლება იყოს როგორც ტექნოლოგიური ასევე ფიზიკური.
- **რა არის SIEM?**
  - SIEM აერთიანებს ინფორმაციული უსაფრთხოების მენეჯმენტსა და ღონისძიების უსაფრთხოების მენეჯმენტს. უზრუნველყოფს უსაფრთოხების გაფრთხიელებების რეალურ დროში ანალიზს ერთ სისტემეაში გაერთაინებულ მონაცემებად. ანუ SEIM გულისხმობს ცალკეული ლოგები შეკრიბოს, დაამუშაოს, გააკეთოს ანალიზი, აღმოაჩინოს ინციდენეტები და შემდეგ მოახდინოს მასზე რეაგირება.
- **რა არის ინფორმაციული უსაფრთხოების მართვის სისტემა?**
  - სისტემური მიდგომა თუ როგორ უნდა იმართებოდეს ინფორმაიცული უსაფრთხოება. ცალკელული აქტივოებები უნდა იმართებოდეს შესაბამისი მიდგომის მიხედვით და ამისთვის მეჯმენტი უნდა იყოს ჩამოყალიბებეული ასევე უნდა იყოს შესაბამისი წესები განსაზღვრული
- **რას ნიშნავს სისუსტეების სკანირება?**
  - პროცესი როდესაც ცალკელი სკანირების მეშვეობით ვახდენთ მოწყვლადობების ანუ სისუსტეების აღმოჩენას და დეტექციას, სისუსტეები წარმოდგენილია cve კოდის მიხედვით სისუსტეების ბაზაში. ასევე თითეულ მოვლენას აქვს თავისი ქულა რომლითაც განვსაზღვრავთ მის დოენს.

ტესტები

- **<u>რას ნიშნავს და რისთვის ხდება ლოგირების გადახესვა?</u>**
  - არის პროცესი როდესაც ხდება გენერირებული ლოგების ანალიზი და მათი დახმარებთ მნიშვნელოვანი მოვლენების გამოკვლევა.
- **<u>რა არის მისაღები გამოყენების პოლიტიკა და ზოგადად პოლიტიკები როგორ მუშავდება და გამოიყენება?</u>**
  - პოლიტიკა არის დოკუმენტი რომელიც ასახავს ორგანიზაციის მისიას მიზნებს და მისწრაფებებს უსაფრთხოების კუტხით
  - მისაღები გამოყენების პოლიტიკა არის დოკუმენტი რომელშიც განსაზღვრულია თუ რა ქმედებები ან პრაქტიკები ითვლება დაუშველად.

- **რას გულისხმობს სისუსტეების CVE და CVSS?**
  - CVSS არის საერთო ქულა რომელიც ენიჭება დაუცველიბას
    - 0.0 არცერთი
    - 0.1 - 3.9 დაბალი
    - 4 - 6.9 საშუალო
    - 7 - 8.9 მაღალი
    - 9 - 10 კრიტიკული
  - CVE არის ყველა საჯაროდ გამჟღავნებული სისუსტეების სია რომელიც მოიცავს CVE ID-ს, აღწერას, თარიღებს და კომენტარებს
- **რა არის ინდიკატორები kpi, kji?**
  - KIP(Key Performance Indicator) გამოიყენება მიზენების მიღწევების შესაფასებლად
  - KJI(Key Job Indicator) მიუთითებს კონკრეტული დავალებების ან სამუშაოების შესრულების ხარისზე ან რაოდენობაზე.
- **რაარის და როგორ მოქმედებს რისკების მართვის ამოცანები ?**
  - ორგანიზაციაში არსებული რისკების იდენტიფიცირებას, შეფასებას და მართვას, რათა ამ რისკების ეფექტი მინიმუმამდე დავიდეს და ორგანიზაციამ შეძლოს მისი მიზნების მიღწევა. რისკების მართვა გულისხმობს
    - რისკების იდენტიფიცირება
    - რისკების შეფასება
    - რიკების პრევენცია
    - რისკების მონიტორინგი
- **აუდიტის კუთხითაც გადავხედოთ თუ რისთვისაა და რატო გამოიყენება?**
  - აუდიტი არის მეთოდური, დამოუკიდებელი, მიუკერძოებელი და დოკუმენტირებული პროცესი რომელის მიზანია მტკიცებულებათა შეგროვება და მათი ობიქტური ანალიზი, აუდიტის კრიტერიუმებთან შესაბამისობაზე.
  - აუდიტის პრიტერიუმებია
    - იუ პოლიტიკა
    - იუმს პროცედურები
    - სტანდარტი (ISO 27001:2013);
    - საკანონმდებლო მოთხოვნები
    - იუმს მოთხოვნები
    - საკონტრაქტო მოთხოვნები
    - დარგობრივ ნორმებს და საუკეთესო პრაქტიკები
    - და ა.შ.
  - აუდიტის პრინციპები
    - კეთილგანწყობა - პროფესიონალიზმის და პატიოსნების დემონსტრირება;
    - კეთილსინდისიერება - სწორი და უშეცდომო სამუშაოს შესრულების ვალდებულება;
    - დეტალურობა და სიზუსტე - აუდიტის გულდასმით გონივრულად შესრულება;

- მიუკერძოებლობა – დამოუკიდებელი და ობიექტური საფუძველი აუდიტის ჩატარების დროს;
- მტკიცებულება – აუდიტის შედეგების ფორმულირების რაციონალური საფუძველი.