**10 ქულიანი თემისთვის**

1. **საბოლოო მოწყობილობები**

ინფორმაციული უსაფრთხოების თვალსაზრისით, საბოლოო მოწყობილობა ეხება ნებისმიერ გამოთვლით მოწყობილობას ან მოწყობილობას, რომელსაც იყენებენ საბოლოო მომხმარებლები ქსელთან ან საინფორმაციო სისტემასთან წვდომისა და ურთიერთქმედების მიზნით. ეს მოწყობილობები, როგორც წესი, მონაცემების საბოლოო დანიშნულებაა და არის ის წერტილები, სადაც მომხმარებლები უშუალოდ ერთვებიან სისტემასთან. ბოლო მოწყობილობები გადამწყვეტი კომპონენტებია საერთო უსაფრთხოების არქიტექტურაში, რადგან ისინი ხშირად მიზნად ისახავს უსაფრთხოების სხვადასხვა საფრთხეებს და დაუცველობას. აქ არის ბოლო მოწყობილობების რამდენიმე ჩვეულებრივი მაგალითი ინფორმაციის უსაფრთხოების კონტექსტში:

* კომპიუტერები და ლეპტოპები: პერსონალური კომპიუტერები და ლეპტოპები არის ძირითადი საბოლოო მოწყობილობები, რომლებსაც ინდივიდები იყენებენ სხვადასხვა ამოცანებისთვის, როგორიცაა ინტერნეტის დათვალიერება, ელ.ფოსტაზე წვდომა და აპლიკაციების გაშვება.
* სმარტფონები და პლანშეტები: მობილური მოწყობილობები სულ უფრო და უფრო პოპულარული ხდება, როგორც ბოლო მოწყობილობები. ისინი უკავშირდებიან ქსელებს უკაბელო ტექნოლოგიების საშუალებით და გამოიყენება კომუნიკაციისთვის, ინტერნეტის დათვალიერებისთვის და მობილური აპლიკაციების გასაშვებად.
* სერვერები: მიუხედავად იმისა, რომ სერვერები, როგორც წესი, განიხილება როგორც სარეზერვო ინფრასტრუქტურის ნაწილად, საბოლოო მოწყობილობები ასევე შეიძლება შეიცავდეს სერვერებს, რომლებიც უშუალოდ ურთიერთობენ საბოლოო მომხმარებლებთან გარკვეულ სცენარებში. მაგალითად, ფაილური სერვერი, რომელიც ინახავს და აზიარებს დოკუმენტებს ლოკალურ ქსელში.
* სამუშაო სადგურები: ორგანიზაციულ გარემოში, თანამშრომლების მიერ გამოყენებული ინდივიდუალური სამუშაო სადგურები განიხილება საბოლოო მოწყობილობებად. ეს შეიძლება შეიცავდეს დესკტოპ კომპიუტერებს ან სპეციალიზებულ სამუშაო სადგურებს სამუშაოს ხასიათიდან გამომდინარე.
* IoT მოწყობილობები: ნივთების ინტერნეტი (IoT) მოწყობილობები, როგორიცაა ჭკვიანი თერმოსტატები, კამერები და სენსორები, სულ უფრო გავრცელებული ხდება, როგორც ბოლო მოწყობილობები. ეს მოწყობილობები ხშირად დაკავშირებულია ქსელებთან და შეიძლება გამოიწვიოს უსაფრთხოების უნიკალური გამოწვევები.
* ქსელური პრინტერები და სკანერები: მოწყობილობები, როგორიცაა პრინტერები და სკანერები, რომლებიც დაკავშირებულია ქსელთან, ასევე განიხილება საბოლოო მოწყობილობებად. ისინი შეიძლება იყვნენ პოტენციური სამიზნეები თავდამსხმელებისთვის, რომლებიც ცდილობენ გამოიყენონ დაუცველობა.

ინფორმაციული უსაფრთხოების საბოლოო მოწყობილობების უსაფრთხოების მოსაზრებები მოიცავს:

* ავთენტიფიკაცია და წვდომის კონტროლი: იმის უზრუნველყოფა, რომ მხოლოდ ავტორიზებულ მომხმარებლებს აქვთ წვდომა მოწყობილობასა და მის რესურსებზე.
* ბოლო წერტილის დაცვა: ანტივირუსული პროგრამული უზრუნველყოფის, ფეიერვოლების და სხვა უსაფრთხოების ზომების დანერგვა მავნე პროგრამებისგან და სხვა საფრთხეებისგან დასაცავად.
* დაშიფვრა: მოწყობილობაზე შენახული და ქსელებით გადაცემული მონაცემების დაშიფვრა, რათა დაიცვას იგი არაავტორიზებული წვდომისგან.
* უსაფრთხოების შესწორება და განახლებები: რეგულარულად განახლდება მოწყობილობის ოპერაციული სისტემა და პროგრამული უზრუნველყოფა ცნობილი დაუცველობის აღმოსაფხვრელად.
* მომხმარებლის განათლება: საბოლოო მომხმარებლების განათლება უსაფრთხოების საუკეთესო პრაქტიკის შესახებ, როგორიცაა საეჭვო ბმულების თავიდან აცილება და ძლიერი პაროლების გამოყენება.
* მოწყობილობის მენეჯმენტი: მოწყობილობების მართვის ცენტრალიზებული გადაწყვეტილებების დანერგვა ორგანიზაციის შიგნით ბოლო მოწყობილობების უსაფრთხოების კონფიგურაციის მონიტორინგისა და კონტროლისთვის.

საბოლოო მოწყობილობების ეფექტურად დაცვა გადამწყვეტია ინფორმაციული სისტემის საერთო უსაფრთხოების შესანარჩუნებლად, რადგან ეს მოწყობილობები ხშირად ემსახურება როგორც შესასვლელ პუნქტს თავდამსხმელებისთვის, რომლებიც ცდილობენ მოიპოვონ არაავტორიზებული წვდომა ან დათრგუნონ მგრძნობიარე მონაცემები.

1. **წვდომის კონტროლები**

წვდომის კონტროლი ეხება მექანიზმებსა და პოლიტიკას, რომლებიც არეგულირებენ წვდომას საინფორმაციო სისტემებზე, რესურსებსა და მონაცემებზე. ეს კონტროლი გადამწყვეტია ორგანიზაციის შიგნით კონფიდენციალურობის, მთლიანობისა და მგრძნობიარე ინფორმაციის ხელმისაწვდომობის შესანარჩუნებლად. წვდომის კონტროლი ინფორმაციული უსაფრთხოების ფუნდამენტური კომპონენტია და მნიშვნელოვან როლს ასრულებს არაავტორიზებული წვდომისა და უსაფრთხოების პოტენციური დარღვევისგან დაცვაში.

არსებობს წვდომის კონტროლის რამდენიმე ტიპი, რომელთაგან თითოეული ემსახურება კონკრეტულ მიზანს რესურსებზე წვდომის მართვისა და შეზღუდვისთვის. წვდომის კონტროლის ძირითადი კატეგორიები მოიცავს:

* 1. ფიზიკური წვდომის კონტროლი:
     + ეს კონტროლი მოიცავს ზომებს შენობებზე, ოთახებსა და აღჭურვილობაზე ფიზიკური წვდომის შეზღუდვის მიზნით.
     + მაგალითებია დაცვის თანამშრომლები, ბიომეტრიული ავთენტიფიკაციის სისტემები, წვდომის ბარათები და სათვალთვალო კამერები.
  2. ლოგიკური ან ტექნიკური წვდომის კონტროლი:
     + ეს კონტროლი ფოკუსირებულია კომპიუტერულ სისტემებზე, ქსელებსა და მონაცემებზე წვდომის კონტროლზე.
     + მაგალითებია პაროლები, დაშიფვრა, ორფაქტორიანი ავთენტიფიკაცია, ბუხარი და შეჭრის აღმოჩენის სისტემები.
  3. ადმინისტრაციული წვდომის კონტროლი:
     + ეს კონტროლი მოიცავს ორგანიზაციის მიერ დადგენილ პოლიტიკას, პროცედურებსა და მითითებებს მომხმარებლის წვდომის სამართავად.
     + მაგალითები მოიცავს მომხმარებლის ანგარიშის მართვას, წვდომის დამტკიცების პროცესებს და უსაფრთხოების შესახებ ინფორმირებულობის ტრენინგს.
  4. როლებზე დაფუძნებული წვდომის კონტროლი (RBAC):
     + RBAC ანიჭებს ნებართვებს მომხმარებლებს ორგანიზაციაში მათი როლების მიხედვით.
     + მომხმარებლებს ენიჭებათ წვდომა მათი სამუშაო პასუხისმგებლობებიდან გამომდინარე, რაც ამცირებს წვდომის არასაჭირო უფლებების რისკს.
  5. ატრიბუტზე დაფუძნებული წვდომის კონტროლი (ABAC):
     + ABAC იყენებს ატრიბუტებს (მომხმარებლის მახასიათებლები, რესურსის თვისებები და გარემო პირობები) წვდომის კონტროლის გადაწყვეტილების მისაღებად.
     + წვდომა მინიჭებულია ან უარყოფილია პოლიტიკის ნაკრების საფუძველზე, რომელიც ითვალისწინებს სხვადასხვა ატრიბუტებს.
  6. სავალდებულო წვდომის კონტროლი (MAC):
     + MAC ახორციელებს წვდომის კონტროლს დაფუძნებული უსაფრთხოების ეტიკეტებზე, რომლებიც დაკავშირებულია საგნებთან (მომხმარებლებთან, პროცესებთან) და ობიექტებთან (ფაილები, მოწყობილობები).
     + გავრცელებულია სამთავრობო და სამხედრო გარემოში, სადაც მონაცემთა კლასიფიკაცია კრიტიკულია.
  7. დისკრეციული წვდომის კონტროლი (DAC):
     + DAC მომხმარებლებს საშუალებას აძლევს გააკონტროლონ წვდომა საკუთარ რესურსებზე, რაც მათ აძლევს დისკრეციას, თუ ვის შეუძლია მათ მონაცემებზე წვდომა.
     + ოპერაციულ სისტემებზე ფაილის ნებართვები DAC-ის ჩვეულებრივი მაგალითია.
  8. დროზე დაფუძნებული წვდომის კონტროლი:
     + ეს კონტროლი ზღუდავს წვდომას გარკვეულ დროზე ან პერიოდზე, რაც ეხმარება ორგანიზაციებს წვდომის მართვაში კონკრეტული დროის ჩარჩოების საფუძველზე.

წვდომის ეფექტური კონტროლი უფრო ფართო უსაფრთხოების სტრატეგიის ნაწილია და ხორციელდება უსაფრთხოების სხვა ზომებთან ერთად ფენიანი თავდაცვის შესაქმნელად. წვდომის კონტროლის პოლიტიკის რეგულარული მიმოხილვები, აუდიტები და განახლებები აუცილებელია უსაფრთხოების მოთხოვნებისა და პოტენციური საფრთხეების ცვლილებებთან ადაპტაციისთვის. წვდომის კონტროლი მნიშვნელოვნად უწყობს ხელს სენსიტიური ინფორმაციის დაცვას და ორგანიზაციის მთლიანი უსაფრთხოების პოზის შენარჩუნებას.

1. **კიბერუსაფრთხოების როლები**

კიბერუსაფრთხოება არის ინფორმაციის უსაფრთხოების კრიტიკული ასპექტი, რომელიც ფოკუსირებულია კომპიუტერული სისტემების, ქსელებისა და მონაცემების დაცვაზე არაავტორიზებული წვდომისგან, თავდასხმებისგან, დაზიანებისგან ან ქურდობისაგან. როგორც ტექნოლოგია აგრძელებს წინსვლას, კიბერუსაფრთხოების მნიშვნელობა სულ უფრო მნიშვნელოვანი ხდება კიბერ საფრთხეების მზარდი რაოდენობისა და დახვეწილობის გამო.

კიბერუსაფრთხოების ძირითადი კომპონენტები ინფორმაციის უსაფრთხოებაში მოიცავს:

1. ქსელის უსაფრთხოება:

* Firewalls: გამოიყენება შემომავალი და გამავალი ქსელის ტრაფიკის მონიტორინგისა და კონტროლისთვის უსაფრთხოების წინასწარ განსაზღვრული წესების საფუძველზე.
* შეჭრის აღმოჩენის სისტემები (IDS) და შეჭრის პრევენციის სისტემები (IPS): აკონტროლეთ ქსელის ან სისტემის აქტივობები მავნე ქმედებებისთვის ან უსაფრთხოების პოლიტიკის დარღვევისთვის.

1. საბოლოო წერტილის უსაფრთხოება:

* ანტივირუსული და ანტიმავნე პროგრამული უზრუნველყოფა: იცავს საბოლოო წერტილებს (კომპიუტერები, სერვერები, მობილური მოწყობილობები) მავნე პროგრამებისგან.
* საბოლოო წერტილის გამოვლენა და რეაგირება (EDR): უზრუნველყოფს რეალურ დროში მონიტორინგს, აღმოჩენას და პასუხს საბოლოო წერტილებზე საფრთხეებზე.

1. პირადობისა და წვდომის მენეჯმენტი (IAM):

* ავთენტიფიკაცია და ავტორიზაცია: უზრუნველყოფს, რომ მხოლოდ ავტორიზებულ პირებს ან სისტემებს აქვთ წვდომა კონკრეტულ რესურსებზე.
* მრავალფაქტორიანი ავთენტიფიკაცია (MFA): მოითხოვს მომხმარებლებს, უზრუნველყონ იდენტიფიკაციის მრავალი ფორმა წვდომის მინიჭებამდე.

1. კრიპტოგრაფია:

* დაშიფვრა და გაშიფვრა: უზრუნველყოფს კომუნიკაციას და მონაცემთა შენახვას ინფორმაციის კოდად გადაქცევით, რომლის გაშიფვრა შესაძლებელია მხოლოდ ავტორიზებული მხარის მიერ.
* ციფრული ხელმოწერები: დაადასტურეთ ციფრული შეტყობინებების ან დოკუმენტების წარმოშობა და მთლიანობა.

1. უსაფრთხოების ინფორმირებულობა და ტრენინგი:

* თანამშრომლების ტრენინგი: ასწავლის მომხმარებლებს კიბერუსაფრთხოების მნიშვნელობის, საერთო საფრთხეებისა და სენსიტიური ინფორმაციის დაცვის საუკეთესო პრაქტიკის შესახებ.

1. ინციდენტზე რეაგირება და მართვა:

* უსაფრთხოების ინციდენტებისა და მოვლენების მენეჯმენტი (SIEM): აგროვებს და აანალიზებს ჟურნალის მონაცემებს უსაფრთხოების ინციდენტების აღმოსაჩენად და რეაგირებისთვის.
* ინციდენტზე რეაგირების გეგმები: ასახავს ნაბიჯებს, რომლებიც უნდა გადაიდგას უსაფრთხოების ინციდენტის დროს, რათა მინიმუმამდე შემცირდეს ზიანი და აღდგენის დრო.

1. დაუცველობის მენეჯმენტი:

* რეგულარული სკანირება და შესწორება: განსაზღვრავს და აგვარებს დაუცველობას პროგრამულ უზრუნველყოფასა და სისტემებში თავდამსხმელების მიერ ექსპლუატაციის თავიდან ასაცილებლად.

1. უსაფრთხოების პოლიტიკა და პროცედურები:

* პოლიტიკის შემუშავება: ადგენს წესებსა და სახელმძღვანელო მითითებებს, რათა უზრუნველყოს უსაფრთხო კომპიუტერული გარემო.
* რეგულარული აუდიტი და შესაბამისობის შემოწმება: უზრუნველყოფს უსაფრთხოების პოლიტიკის დაცვას და სისტემების შესაბამის რეგულაციებს.

1. უსაფრთხო პროგრამული უზრუნველყოფის განვითარება:

* კოდირების უსაფრთხო პრაქტიკა: უზრუნველყოფს პროგრამული უზრუნველყოფის შემუშავებას უსაფრთხოების გათვალისწინებით დაუცველობის თავიდან ასაცილებლად.
* კოდების მიმოხილვა და ტესტირება: განსაზღვრავს და აგვარებს უსაფრთხოების ხარვეზებს პროგრამულ უზრუნველყოფაში განთავსებამდე.

1. ღრუბლოვანი უსაფრთხოება:

* უსაფრთხო კონფიგურაცია: უზრუნველყოფს ღრუბლოვანი სერვისების და ინფრასტრუქტურის უსაფრთხოდ კონფიგურაციას.
* მონაცემთა დაშიფვრა: იცავს ღრუბელში შენახულ მონაცემებს არაავტორიზებული წვდომისგან.

კიბერუსაფრთხოება არის დინამიური და განვითარებადი სფერო, სადაც ორგანიზაციები მუდმივად ერგებიან ახალ საფრთხეებსა და ტექნოლოგიებს. უწყვეტი მონიტორინგი, საფრთხის დაზვერვა და თანამშრომლობა კიბერუსაფრთხოების საზოგადოებაში აუცილებელია პოტენციური რისკების წინ დარჩენისთვის.

1. **სოციალური ინჟინერია**

სოციალური ინჟინერია გულისხმობს ინდივიდების მანიპულირებას, რათა მიიღონ წვდომა ინფორმაციაზე ან სისტემებზე. ეს არის არატექნიკური მეთოდი, რომელსაც იყენებენ თავდამსხმელები ადამიანის ფსიქოლოგიის გამოსაყენებლად, ვიდრე კოდის ან დახვეწილი ჰაკერების ტექნიკის გამოყენებისას. თავდამსხმელები იყენებენ სხვადასხვა ფსიქოლოგიურ ხრიკებს, რათა მოატყუონ ადამიანები კონფიდენციალური ინფორმაციის გამჟღავნებაში, მოქმედებების შესრულებაში ან უსაფრთხო სისტემებზე წვდომის მიცემის მიზნით.

სოციალური ინჟინერიის შეტევების რამდენიმე ტიპი არსებობს:

1. ფიშინგი: თაღლითური ელფოსტის ან შეტყობინებების გაგზავნა, რომლებიც, როგორც ჩანს, ლეგიტიმური წყაროებიდან არის, რათა მოატყუონ პირები, რათა გამოავლინონ მგრძნობიარე ინფორმაცია, როგორიცაა პაროლები, საკრედიტო ბარათის ნომრები ან პერსონალური მონაცემები.
2. პრეტექსტინგი: შეთითხნილი სცენარის შექმნა სამიზნედან ინფორმაციის მისაღებად. მაგალითად, თავდამსხმელმა შეიძლება წარმოაჩინოს როგორც ავტორიტეტი, როგორიცაა IT ტექნიკოსი ან თანამშრომელი, ინფორმაციის შეგროვებისთვის.
3. Baiting: პიროვნებების მოზიდვა რაღაც სასურველით, როგორიცაა უფასო პროგრამული უზრუნველყოფის ჩამოტვირთვა ან USB დისკი, რომელიც შეიცავს მავნე პროგრამას ან ვირუსს. მას შემდეგ, რაც მსხვერპლი გამოიყენებს სატყუარას, მათი სისტემა კომპრომეტირებული ხდება.
4. Quid pro quo: მომსახურების ან სარგებლის შეთავაზება ინფორმაციის სანაცვლოდ. მაგალითად, თავდამსხმელმა შეიძლება წარმოადგინოს ტექნიკური მხარდაჭერა და შესთავაზოს დახმარება შესვლის სერთიფიკატების სანაცვლოდ.
5. კუდი: ფიზიკური მიდევნება შეზღუდულ ზონაში სათანადო ნებართვის გარეშე. ეს ხშირად ხდება ოფისის პარამეტრებში, სადაც თავდამსხმელი იძენს წვდომას დაცულ ადგილებში თანამშრომლის მჭიდრო თვალყურის დევნით.

სოციალური ინჟინერიის თავდასხმები ეყრდნობა ადამიანის ქცევის ექსპლუატაციას, ხშირად იყენებს ნდობას, ავტორიტეტს, სასწრაფოობას ან ცნობისმოყვარეობას, რათა მანიპულირებდეს მსხვერპლზე წვდომის ან ინფორმაციის მიწოდებაში. ორგანიზაციები ებრძვიან ამ შეტევებს თანამშრომელთა ტრენინგის, ცნობიერების ამაღლების პროგრამებისა და უსაფრთხოების პროტოკოლების დანერგვით, წვდომის მოთხოვნების ავთენტიფიკაციისა და მგრძნობიარე მონაცემების დასაცავად.

**3 ქულიანი ღია კითხვები**

1. **შიფრაციასთან დაკავშირებით**

დაშიფვრა არის ინფორმაციის უსაფრთხოებისა და კონფიდენციალურობის გადამწყვეტი ასპექტი, რომელიც მნიშვნელოვან როლს ასრულებს სენსიტიური მონაცემების არაავტორიზებული წვდომისგან დაცვაში. იგი მოიცავს უბრალო ტექსტის (წაკითხვადი მონაცემების) დაშიფვრულ ტექსტად (წაკითხვადი მონაცემები) გადაქცევის პროცესს ალგორითმისა და საიდუმლო გასაღების გამოყენებით. დაშიფვრის მიზანია ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ზოგჯერ ავთენტურობის უზრუნველყოფა.

აქ მოცემულია რამდენიმე ძირითადი კონცეფცია, რომელიც დაკავშირებულია დაშიფვრასთან:

დაშიფვრის ტიპები:

* **სიმეტრიული დაშიფვრა:** სიმეტრიული გასაღების დაშიფვრისას, იგივე გასაღები გამოიყენება როგორც დაშიფვრის, ასევე გაშიფვრის პროცესებისთვის. მაგალითები მოიცავს Advanced Encryption Standard (AES) და Data Encryption Standard (DES).
* **ასიმეტრიული დაშიფვრა:** ასიმეტრიული გასაღების დაშიფვრა იყენებს საჯარო და კერძო გასაღებების წყვილს. საჯარო გასაღებით დაშიფრული მონაცემების გაშიფვრა შესაძლებელია მხოლოდ შესაბამისი პირადი გასაღებით და პირიქით. საერთო ალგორითმები მოიცავს RSA და Elliptic Curve Cryptography (ECC).
* **ჰეშის ფუნქციები:** ჰეშის ფუნქციები არის ცალმხრივი მათემატიკური ალგორითმები, რომლებიც გარდაქმნის მონაცემებს სიმბოლოების ფიქსირებული ზომის სტრიქონად, რომელიც, როგორც წესი, არის ჰეშის მნიშვნელობა ან დაიჯესტი.

ისინი ჩვეულებრივ გამოიყენება მონაცემთა მთლიანობის შესამოწმებლად. თუ ორიგინალური მონაცემები შეიცვლება, ჰეშის მნიშვნელობაც შეიცვლება.

* **გასაღების მენეჯმენტი:** დაშიფვრის გასაღებების უსაფრთხო მართვა გადამწყვეტია. თუ არაავტორიზებული მხარე მიიღებს წვდომას გასაღებზე, მათ შეუძლიათ დაშიფრული მონაცემების გაშიფვრა.

გასაღების განაწილება, შენახვა და როტაცია გასაღების ეფექტური მართვის ძირითადი ასპექტებია.

* **საჯარო გასაღების ინფრასტრუქტურა (PKI):**

PKI არის სისტემა, რომელიც მართავს ციფრულ გასაღებებს და სერთიფიკატებს. იგი ჩვეულებრივ გამოიყენება ასიმეტრიულ დაშიფვრაში უსაფრთხო კომუნიკაციისა და ციფრული ხელმოწერებისთვის.

* **დაშიფვრის აპლიკაციები:**

უსაფრთხო კომუნიკაცია: დაშიფვრა ფართოდ გამოიყენება ინტერნეტის საშუალებით კომუნიკაციის უზრუნველსაყოფად, როგორიცაა HTTPS უსაფრთხო ვებ დათვალიერებისთვის.

* **მონაცემთა დასვენების დროს დაცვა:** დაშიფვრა იცავს მოწყობილობებზე ან სერვერებზე შენახულ მონაცემებს, იცავს მათ არაავტორიზებული წვდომისგან ქურდობის ან დაკარგვის შემთხვევაში.
* **ავთენტიფიკაცია:** ციფრული ხელმოწერები იყენებს ასიმეტრიულ დაშიფვრას შეტყობინების ან დოკუმენტის ავთენტურობის შესამოწმებლად.
* **გამოწვევები:** გასაღებების უსაფრთხოდ მართვის გამოწვევა.

ძლიერი დაშიფვრის საჭიროების დაბალანსება სისტემების შესრულების მოთხოვნებთან.

დაშიფვრის ალგორითმებში პოტენციურ დაუცველობასთან გამკლავება.

* **კვანტური გამოთვლა და პოსტ-კვანტური კრიპტოგრაფია:** კვანტური კომპიუტერების განვითარება პოტენციურ საფრთხეს უქმნის დაშიფვრის ალგორითმებს. მკვლევარები მუშაობენ პოსტ-კვანტურ კრიპტოგრაფიაზე, რათა განავითარონ ალგორითმები, რომლებსაც შეუძლიათ წინააღმდეგობა გაუწიონ კვანტურ შეტევებს.
* **მარეგულირებელი შესაბამისობა:** სხვადასხვა რეგულაციები და სტანდარტები, როგორიცაა GDPR (General Data Protection Regulation) და HIPAA (ჯანმრთელობის დაზღვევის პორტაბელურობისა და ანგარიშვალდებულების აქტი), ავალდებულებს დაშიფვრის გამოყენებას მგრძნობიარე ინფორმაციის დასაცავად.

1. **CIA ტრიადა**

CIA ტრიადა არის ინფორმაციული უსაფრთოხების ცალკეული ორგანიზაციების კონტროლის მექანიზმი, რომელიც განახორციელებს უსაფრთხოების ზომების თავისანაათებს. ის შეიცავს 3 კომპონენტს ესენია:

კონფიდენციალურობა: ინფორმაციის დაცვა არავტორიზირებული წვდომისგან,

მთლიანობა: არ შეიცვალოს მონაცემები არავტორიზირებული მხარის მხირდან,

ხელმისაწვდომობა: ინფორმაციაზე წვდომა ნობისმიერ დროს ავტორიზირებული მომხმარებლისთვის.

CIA Triad არის ინფორმაციული უსაფრთხოების ფუნდამენტური მოდელი, რომელიც ასახავს სამ ძირითად პრინციპს, რომელიც აუცილებელია უსაფრთხოების პოლიტიკის შემუშავებისა და განხორციელებისთვის. აკრონიმის თითოეული ასო წარმოადგენს ინფორმაციის უსაფრთხოების ფუნდამენტურ ასპექტს:

* 1. **კონფიდენციალურობა:** ეს ეხება სენსიტიური ინფორმაციის დაცვას არაავტორიზებული წვდომისგან ან გამჟღავნებისგან. ის გულისხმობს იმის უზრუნველყოფას, რომ მხოლოდ ავტორიზებულ პირებს ან სისტემებს შეუძლიათ წვდომა გარკვეულ მონაცემებსა და რესურსებზე.
  2. **მთლიანობა:** მთლიანობა ფოკუსირებულია მონაცემთა სანდოობასა და სიზუსტეზე. იგი მოიცავს მონაცემთა თანმიმდევრულობის, სანდოობისა და სანდოობის შენარჩუნებას მისი მთელი სიცოცხლის ციკლის განმავლობაში. ეს პრინციპი უზრუნველყოფს, რომ მონაცემები დარჩეს უცვლელი და დაუცველი შენახვის, დამუშავებისა და გადაცემის დროს.
  3. **ხელმისაწვდომობა:** ხელმისაწვდომობა ხაზს უსვამს საჭიროების შემთხვევაში მონაცემთა და რესურსების ხელმისაწვდომობას. ის უზრუნველყოფს ავტორიზებული მომხმარებლების დროულ და შეუფერხებელ წვდომას ინფორმაციასა და სერვისებზე. ეს პრინციპი მოიცავს ღონისძიებების განხორციელებას, რათა თავიდან იქნას აცილებული და შემცირდეს შეფერხებები, რამაც შეიძლება გამოიწვიოს შეფერხება ან მომსახურების უარყოფა.

1. **მავნე პროგრამული უზრუნველყოფები malware**

მავნე პროგრამა, მოკლედ მავნე პროგრამული უზრუნველყოფისთვის, ეხება ნებისმიერ პროგრამულ უზრუნველყოფას, რომელიც სპეციალურად შექმნილია კომპიუტერული სისტემების, ქსელების ან მომხმარებლების დასაზიანებლად ან გამოსაყენებლად. მავნე პროგრამული უზრუნველყოფა იქმნება მავნე განზრახვით და მას შეუძლია მიიღოს სხვადასხვა ფორმები, მიზნად ისახავს შეაფერხოს, დააზიანოს ან მოიპოვოს არაავტორიზებული წვდომა კომპიუტერულ სისტემებსა და მგრძნობიარე ინფორმაციაზე.

აქ არის მავნე პროგრამების რამდენიმე გავრცელებული ტიპი:

* 1. ვირუსები: ეს არის პროგრამები, რომლებსაც შეუძლიათ გამრავლება და გავრცელება სხვა პროგრამებზე მიმაგრებით. მათ შეუძლიათ დააზიანონ ან გააფუჭონ ფაილები და ხშირად საჭიროებენ მომხმარებლის ინტერაქციას გავრცელებისთვის.
  2. Worms: Worms არის თვითგანმეორებადი პროგრამები, რომლებიც შეიძლება გავრცელდეს ქსელებში მომხმარებლის ყოველგვარი ურთიერთქმედების გარეშე. ისინი იყენებენ დაუცველობას ქსელის პროტოკოლებში გასავრცელებლად და შეუძლიათ მნიშვნელოვანი ზიანი მიაყენონ სისტემებს.
  3. ტროიანები: ბერძნულ მითოლოგიაში ცნობილი ხის ცხენის სახელით დასახელებული, ტროას მატყუარა პროგრამებია, რომლებიც ლეგიტიმურად გამოიყურება, მაგრამ შეიცავს მავნე კოდს. გააქტიურების შემდეგ მათ შეუძლიათ შეასრულონ სხვადასხვა მავნე მოქმედებები, როგორიცაა სენსიტიური ინფორმაციის მოპარვა ან სისტემაში არაავტორიზებული წვდომის უზრუნველყოფა.
  4. Ransomware: ამ ტიპის მავნე პროგრამა შიფრავს მომხმარებლის ფაილებს ან მთელ სისტემას, რაც მათ მიუწვდომელს ხდის. შემდეგ თავდამსხმელები გამოსასყიდს ითხოვენ გაშიფვრის გასაღების მიწოდების სანაცვლოდ. გამოსასყიდი პროგრამების შეტევები სულ უფრო ხშირად ხდება და შეიძლება მძიმე შედეგები მოჰყვეს ინდივიდებსა და ორგანიზაციებს.
  5. Spyware: Spyware შექმნილია მომხმარებლის საქმიანობის შესახებ ინფორმაციის ფარულად მონიტორინგისა და შეგროვების მიზნით, მათი ცოდნისა და თანხმობის გარეშე. ეს ინფორმაცია შეიძლება შეიცავდეს კლავიშების დაჭერას, შესვლის სერთიფიკატს და დათვალიერების ჩვევებს, რომლებიც შეიძლება გამოყენებულ იქნას სხვადასხვა მავნე მიზნებისთვის.
  6. Adware: მიუხედავად იმისა, რომ არ არის ისეთივე მავნე, როგორც სხვა სახის მავნე პროგრამები, adware აჩვენებს არასასურველ რეკლამებს მომხმარებლის მოწყობილობაზე, რაც ხშირად არღვევს მომხმარებლის გამოცდილებას და ზოგჯერ იწვევს კონფიდენციალურობის პრობლემებს.

მავნე პროგრამების გავრცელება შესაძლებელია სხვადასხვა საშუალებებით, როგორიცაა ინფიცირებული ელ.ფოსტის დანართები, მავნე ვებსაიტები, კომპრომეტირებული პროგრამული უზრუნველყოფა ან ოპერაციული სისტემებისა და აპლიკაციების დაუცველობების გამოყენება. მავნე პროგრამებისგან თავის დასაცავად აუცილებელია განახლებული ანტივირუსული და მავნე პროგრამების გამოყენება, ოპერაციული სისტემებისა და აპლიკაციების შენახვა და უსაფრთხო გამოთვლითი ჩვევების გამოყენება, როგორიცაა საეჭვო ჩამოტვირთვებისა და ელფოსტის დანართების თავიდან აცილება.

1. რა არის ინფორმაცია? განიხილეთ მისი კლასიფიკაცია.

ინფორმაცია არის დამუშავებული მონაცემების ერთობლიო როგორიცაა ფაქტები, ციფრები, დოკუმენტები, სურათები ან თუნდაც ხმის ჩანაწერები რომელიც ატარებს კონკრეტულ მნიშვენოლბას და გააჩნია მიზანი. მისი წარმოდგენა შეიძლება მატერიალურად და ასევე ციფრულად.  
რაც შეეხება კლასიფიკაციას ესენია, კრიტიკული ინფორმაციული სისტემა რომელიც გულისხმობს ინფორმაციულ უწყვეტობას ქვენის სხვადასხვა სექტორის ნორმალურად ფუნქციონირებისთვის. ასევე კომფიდენციაურლი ინფორმაცია, ის წარმოპადგენს ინფორმაციას რომლიც არის წარმოდგენილი დოკუმენტის ან ელექტრონული ფორმით, მისი გამჟღავნება საფრთხეს შეუქმნის ორგანიზაციას. შინაგან სამსახურერივი გამოყენების ინფორმაცია რომელიც წარმოდგენს ხეშეკრულებას თანამშრომელბსა და ორგანიზაციას შორის. ინფორმაციულიო აქტივი ეს არის ორგანიზაციაში არსებული ინფორმაციის ერთობლიობა რომლის გამოყენებითაც შესაძლებელია ინფორმაციის გაზრდა დაცვა გაგება და ეფექტური გამოყენება. ეს შეიძლება იყოს ფლეშ მეხსიერება, დიკი, სერვერი, ნივთები, თანამშორმლები, კომპიუტერები და სხვა. ინფორმაციული სისტემა ეს არის მოქმედების განხორციელება ტექნოლოგიების გამოყენებიტ ინფორმაციის სამართავად.

1. ახსენით ინფორმაციული უსაფრთხოების პრინციპები და პოლიტიკა.

ინფოტმაიული უსაფრთხოება ეს არის ინფორმაციის უნებართვოდ წვდომისგან დასაცვისთვის შემნილი პროეცესებისა და მიდგომების ერთობლიობა.   
  
ინფორმაციის უსაფრთხოების პრინციპებია:  
კომფიდენციალურიბა: ინფორმაციის უკანონო გამჟღავნებისგან დაცვა .

მთლიანობა: ინფორმაციის სისრულის მახასიათებელი.

ხელმისაწვდომობა: ინფორმაციაზე წვდომა შეუფერხებლად უფლება მოსილი პირებისთვის.

1. რა არის რისკი და როგორ ხდება მისი იდენტიფიცირება?

აქტივების კომფიდენციალურობის, მთლიანიბოს ან ხელმისაწვდომობის დარღვევის ალბათობა.   
რისკის იდენტიფიცირება გულისხმობს აქტივების საფრთხეების მონიტორინგს მის იდენტიფიცრებას და შეფასებას რათა შემდეგ დაინერგოს მისი შერბილების სტარტეგია.

1. რა არის CIA ტრიადა?

CIA ტრიადა არის ინფორმაციული უსაფრთოხების ცალკეული ორგანიზაციების კონტროლის მექანიზმი, რომელიც განახორციელებს უსაფრთხოების. ის შეიცავს 3 კომპონენტს ესენია:

* **კონფიდენციალურობა:** ინფორმაციის დაცვა არავტორიზირებული წვდომისგან,
* **მთლიანობა:** არ შეიცვალოს მონაცემები არავტორიზირებული მხირდან,
* **ხელმისაწვდომობა:** ინფორმაციაზე წვდომა ნობისმიერ დროს ავტორიზირებული მომხმარებლისთვის.

1. რა აირს SOC?

ეს არის უსაფრთხოების ოპერაციების ცენტრი რომელის მიზანია კიბერ უსაფრთხოების მონიტორინგი, მისი პრევენცია, გამოვლენა და რეაგირება. მათ ევალებათ ორგანიზაციების აქტივების მონიტორინგი და დაცვა.

1. რა არის Sniffing და Spoofing?

Sniffing და spoofing ტექნიკები გამოიყენება კიბერშეტევებში ქსელის ტრაფიკის ჩარევისა და მანიპულირებისთვის.  
Sniffing კონკრეტულად არის პასიური ქსელის მონიტორინგის ტექნიკა რომლის დროსაც თავმდამსხმელი ძირითადად არაავტორიზირებული გზით იღებს და აანალიზებს ქსელსი ტრაფიკს. ამ ტექნიკის მიზანია გადაცემული მონაცემების მოსმენა ისე რომ ქსელის ტაფიკი არ შეფერხდეს. Sniffing-სიგანე თავის დასაცავად გამოიტენება დაშიფრის ტექნიკები როგორიცაა VPN ან SSL/TLS.

Spoofing არის აქტიური ქსელის შეტევა, რომლის დროსაც თავდამსხმელი ასახავს სხვა ერთეულს მაგალითად ლეგიტიმური მომხამრებელს, მოწყობილობას ან სერვერს რათა მოიპოვოს არაავტორიზირებადი წვდომა ან მანიპულაცია მოახდინოს ქსელის ტრაფიკზე. Spoofing-ის დროს თავმდამსხმელები ცვლიან წყაროს IP მისამართებს რათა ისე გამოჩნდეს თითქოს ტაფიკი მოდის სანდო წყაროსგან ამას კი IP Address Spoofing-ს უწოდებენ. ასევე არსეობს DNS Spoofing როდესაც ხდებს DNS -ის გაყალბება. MAC Address Spoofing-ის დროს კი თავდმამსხმელები MAC მისამართს ცვლიან სხვა მოწობილობის იმიტაციისთვის. კიდევ არსებობს სხბა ტიპები spoofing-ის რომლებიც ასევე ემსახურებიან გაყალბების ხარჯე მონაცემებეის მოპარვას.

1. რა არის IP დაუცველობა?  
     
   IP (ინტერნეტ პროტოკოლის) დაუცველობა ეხება სისუსტეებს ან ხარვეზებს IP პროტოკოლის იმპლემენტაციაში. IP დაუცველობა მოიცავს: IP Spoofing-ს რაც გულისხმობს იმას რომ თავდამსხმელებს შეუძლიათ გააყალბონ წყაროს IP მისამართები რათა თავი წარმოაშინონ სანდო სუბეიქტად, ეს კი თავისმხრივ ნიშნავს არაავტორიზირებულ წვდომას და ტრაფიკზე მანიპულაციას, ასევე IP Fragmentation Attacks როელმაც შეიძლება გამოიწვიოს რესურსების ამოწუვა და უსაფრთოების ზომების თავიდანა ცილება. IP Routing Attacks-ის დროს კი თავდმასხმელმა შეიძლება მარშუტიზაციაზე მოახდინოს მანიპულაციამარშუტის ოქმების BGP-სი გამოყენებით რამაც შეიძლება გამოიწვიოს ტრაფიკის ჩაჭრა. IPSEC Vulnerabilities არის IPის ერთ ერთი დაცუველოსბის სახე მართალია IPSEC გამოიყენება უსაფრთხო კომუნიკაციისთვსი მაგრამ მის არასწორმა დაკომფიგურიებამ შეიძლება გამოწვიოს უსაფრთხოებასთან დაკავშირებული პრობლემები.

      3. რა არის TCP/UDP დაუცველობა?

TCP (Transmission Control Protocol) და UDP (User Datagram Protocol) არის ძირითადი პროტოკოლები, რომლებიც გამოიყენება მოწყობილობებს შორის ინტერნეტით კომუნიკაციისთვის.

TCP:

TCP/IP Stack Exploits დაუცველობის დროს ოპერაციული სისტემების TCP / IP დასტის დაუცველობა ქმნის შესაძლებლობას დისტანციური კოდის შესრულებისთვის ან DoS შეტევებისთვის.  
TCP Sequence Number Predictability: პროგნოზირებადი თანმიმდევრობის ნომრების გამოყენება შესაძლებელია თავდამსხმელების მიერ მავნე მონაცემების TCP ნაკადებში შესაყვანად.

UDP:

თავდამსხმელები აგზავნიან მცირე UDP მოთხოვნებს სერვერების გასახსნელად, როგორიცაა DNS ან NTP სერვერები, spoofed source IP მისამართებით ამას კი UDP Amplification Attacks-ს უწოდებენ, ასევე არსებოსბPacket Loss რომლის დროსაც UDP– ს არ გააჩნია შეცდომების გამოვლენისა და კორექტირების მექანიზმები, რაც მას მგრძნობიარეს ხდის პაკეტის დაკარგვისა და მონაცემთა კორუფციის მიმართ.

ინფორმაციის უსაფრთოებისთვის უდიდეს როდს თამაშობს მონაცმეების დაშიფრა, ასევე ნდობა უმნიშვენლოვანესია ციფრულ სამყაროში, ამიტომ ციფრული სერთიფიკატები და ამით გამყარებული ნდობა არის ფუნდამენტური ნაწილი ინფორმაციულ უსადრთხობაში, შესაბამისად ამ ყოველივეს გაგება თუ როგორ მუშაობს და რას წამოადგენს ასევე მნიშვენლოვანია.  
  
სიმეტრიული დაშიფვრა გულისხმობს ერთი გასაღების გამოყენებას მონაცემთა როგორც დასაშიფრად ასევე გასაშიფრად. საგულისხმოა რომ  სიმეტრიული დაშიფვრის უპირველესი პრობლემა მდგომარეობს იმაში, რომ გასაღების უსაფრთხოდ გაზიარება კომუნიკაციის მხარეებს შორის ძალიან რთულია.

ასიმეტრიული დაშიფვრა, სიმეტრიულისგან განსხვავებით მუშაობს წყვილი გასაღებებით: საჯარო გასაღები (Public Key) და პირადი გასაღები (Private Key). საჯარო გასაღები ხელმისაწვდომია ყველასთვის და გამოიყენება დაშიფვრისთვის, ხოლო პირადი გასაღები, რომელიც საიდუმლოდ ინახება მფლობელთან გამოიყენება გაშიფვრისთვის. ეს სისტემა უზრუნველყოფს უსაფრთხო კომუნიკაციას გასაღების წინასწარ გაცვლის გარეშე. ცნობილი ასიმეტრიული დაშიფვრის ალგორითმებს წარმოადგენს RSA (Rivest-Shamir-Adleman) და Elliptic Curve Cryptography (ECC).

რაც შეეხება ციფრული სერთიფიკატების, ეს გადამწყვეტ როლს თამაშობს ონლაინ კომუნიკაციების ავთენტურობისა და მთლიანობის უზრუნველსაყოფად. ეს სერთიფიკატები გაცემულია სერტიფიკატების ორგანოების (CA) მიერ და შეიცავს ინფორმაციას, რომელიც ადასტურებს ვებსაიტის ან პირის ვინაობას. ისინი აკავშირებენ საჯარო გასაღებს ერთეულის იდენტობასთან, ამყარებენ ნდობას და უზრუნველყოფენ უსაფრთხო კავშირებს ინტერნეტით. ციფრული სერთიფიკატები იყენებენ კრიპტოგრაფიულ ხელმოწერებს მათი ლეგიტიმურობის დასადასტურებლად, რათა თავიდან აიცილონ არაავტორიზებული ცვლილებები.

PKI იგივე საჯარო გასაგების უნფრასტრუქტურა ემსახურება ციფრული სერთიფიკატების მართვისა და საჯარო გასაღების დაშიფვრის ჩარჩოს. იგი მოიცავს პროცედურებს, აპარატურას, პროგრამულ უზრუნველყოფას და ადამიანებს, რომლებიც ერთად მუშაობენ ინფორმაციის გაცვლის უსაფრთხო ინფრასტრუქტურის უზრუნველსაყოფად. PKI იძლევა ციფრული სერთიფიკატების შექმნას, განაწილებას და მართვას. ის უზრუნველყოფს უსაფრთხო კომუნიკაციას და იდენტურობის დადასტურებას სხვადასხვა აპლიკაციებში, როგორიცაა უსაფრთხო ბრაუზინგი, ელფოსტის დაშიფვრა და ციფრული ხელმოწერები.  
  
საერთო ჯამში ეს კომპონენტები ქმნიან უსაფრთხო გარემოს ფიცრულ სამყაროში, რომელიც იცავს ადამიანებს უსაფრთხოების დარღვევისგან.

**Malware** არის მავნე პროგრამული უზრუნველყოფა, როგორიცაა ვირუსები, trojanები და სხვა , რომელსაც შეუძლია დააინფიციროს სისტემა და გამოიწვიოს ზიანი ან მოიპაროს ინფორმაცია.

არსებობს 4 სახის ძირითადი მალვეარები: **trojans, spyware, viruses, and ransomware.**

**Trojan -**არის სოფტვეარი რომელიც ‘’ასაღებს’’ თავს როგორც რეალური პროგრამად, რითაც ატყუებს მომხმარებლებს რომ გადმოიწერონ იგი, რომლის დაინსტალირების შემდეგაც იგი, იუზერისგან არაცნობიერად აინსტალირებს keyloggerს, ვირუსებს, აკეთებს ბექდორ ექსესს დივაისთან და შეიძლება მოიპაროს იუზერის პირადი ინფორმაციაც კი.

**Spyware** - კომპიუტერზე ან მობილურ მოწყობილობაზე განხორციელებისას, ჯაშუშური პროგრამა აგროვებს ინფორმაციას ადამიანების ან ორგანიზაციების შესახებ მომხმარებლის აქტივობის მონიტორინგით და თავდამსხმელის შესახებ მოხსენების გზით , მას შეუძლია მოიპოვოს იუზერნეიმები, პასვორდები, ბარათის ინფორმაციები და ა.შ

**Viruses** - ვირუსები არის თვითგანმეორებადი მავნე კოდი, რომელსაც შეუძლია სხვა პროგრამების დაინფიცირება და სისტემებში გავრცელება. პარაზიტის მსგავსად, ვირუსი ეყრდნობა მასპინძელ აპლიკაციას, რათა გავრცელდეს, გაიშვას და გამრავლდეს მხოლოდ ინფიცირებული აპლიკაციის მუშაობის დროს.

**Ransomware** - არის მავნე პროგრამა, რომელიც შიფრავს ფაილებს ან მოწყობილობებს და შიფრავს მათ მხოლოდ მას შემდეგ, რაც კომპანია შეასრულებს მოთხოვნილ გამოსასყიდის გადახდას

**ფიშინგი** - სოციალური ინჟინერიის შეტევის ტიპი, სადაც თავდამსხმელები იყენებენ ყალბ ელ.წერილს ან ვებსაიტებს, რათა მოატყუონ მომხმარებლები სენსიტიური ინფორმაციის გასაჯაროებაში ან მავნე პროგრამების ჩამოტვირთვის მიზნით. ფიშინგ მესიჯმა შესაძლოა ვინმე დაარწმუნოს რომ შეასრულოს რამე ქმედება, მაგალითად დააინსტალიროს საეჭვო მალვეარი და ამით მოახდინოს ათაქერმა დისტანციური დაკავშირება. მეილის დახმარებით შესაძლებელია ფეიკ ბანკის ან ი-კომერს საიტის დაფეიკება და მოწყვლად ხალხთან მისი გაგზავნა, მესიჯით რომ ვინმე ცდილობს დაჰაკოს მისი საბანკო ანგარიში ან რამე, და ეს რომ თავიდან აირიდოს უგზავნის ლინკს რომელიც რეალურად არის სპუფინგ საიტი, და იქ რომ შევა და ავტორიზაციით დააქონექთებს თავის ექაუნთზე, მაგ დროს მოხდება პირადი ინფორმაციის მოპარვა.

ფიშინგის სახეებია: whaling, spear phishing, email phishing რომელიც ზევით მიწერია.

**Distributed Denial of Service (DDoS)**: შეტევა, რომელიც უტევს ქსელს ან სერვერს ტრაფიკით, რათა გადაიტვირთოს იგი და გამოიწვიოს მისი შეფერხება ან გახადოს მიუწვდომელი. ზოგიერთი ტიპის DDoS შეტევები უბრალოდ მიზნად ისახავს ქსელის გამტარუნარიანობის მოხმარებას, უარყოფს მას ლეგიტიმურ მასპინძლებს, ბოტების დიდი რაოდენობის გამოყენებით. სხვები იწვევენ რესურსების ამოწურვას ჰოსტების დამუშავების მოთხოვნებზე, მოიხმარენ CPU ციკლებს და მეხსიერებას. ეს აჭიანურებს ლეგიტიმური ტრაფიკის დამუშავებას და შესაძლოა მასპინძელი სისტემა მთლიანად დაზიანდეს. მაგალითად მოვიყვანოთ, 2008 წლის ომის დროს ჰაკები, ან პროსერვისზე 2019 წელს მიტანილი იერიშები.

**დაზვერვითი თავდასხმები** ეხება კიბერშეტევის ტიპს, სადაც დამნაშავე ცდილობს შეაგროვოს მგრძნობიარე ინფორმაცია, მონაცემები ან დაზვერვა სამიზნე ინდივიდის, ორგანიზაციის ან სამთავრობო ერთეულის შესახებ. სადაზვერვო შეტევების მიზანი შეიძლება განსხვავდებოდეს და შეიძლება მოიცავდეს კორპორატიულ ჯაშუშობას, ფინანსურ თაღლითობას, ინტელექტუალური საკუთრების ქურდობას ან თუნდაც სახელმწიფოს მიერ დაფინანსებულ ჯაშუშობას. ეს თავდასხმები ხშირად მოიცავს ისეთი მოწინავე ტექნიკის გამოყენებას, როგორიცაა სოციალური ინჟინერია, ფიშინგი, მავნე პროგრამები და კიბერ ექსპლუატაციის სხვა ფორმები სენსიტიური ინფორმაციისთვის არაავტორიზებული წვდომის მოსაპოვებლად.

სადაზვერვო თავდასხმებს შეიძლება სერიოზული შედეგები მოჰყვეს, დაწყებული ფინანსური ზარალით, რეპუტაციის ზარალით, ინტელექტუალური საკუთრების დაკარგვით და ეროვნული უსაფრთხოების საფრთხეც კი. როგორც ასეთი, მნიშვნელოვანია ორგანიზაციებმა და ინდივიდებმა გადადგან პროაქტიული ნაბიჯები ამ ტიპის თავდასხმებისგან თავის დასაცავად, მათ შორის ძლიერი კიბერუსაფრთხოების ზომების განხორციელება, თანამშრომლების ტრენინგი პოტენციური საფრთხეების იდენტიფიცირებისა და რეაგირების შესახებ და მათი ქსელების მონიტორინგი ნებისმიერი საეჭვო აქტივობისთვის.

**კიბერსაფრთხეები** შეიძლება იყოს მრავალი სახის, რომელიც მიუთითებს კიბერუსაფრთხოების ისეთ პროდუქტებზე, სერვისებზე, ქსელებზე, სისტემებსა და ინფორმაციაზე კიბერშეტევის საფრთხის შესახებ. კიბერ საფრთხეები შეიძლება იყოს: malware, ვირუსები, ჰაკინგი, ფიშინგი და კიბერთავდასხმები.

**სოციალური ინჟინერია:** სოცაილური ინჟინერია არის ტექნიკა რომელიც აგამოიყენებათავდამსხმელების მიერ ადამიანებზე ზეწოლისთვის და ინდივიდუალების მოსატყუებლას რომ მოიპოვონ სენსიტუიური ინფორმაცაია მოქმედებების შესრულება, რომლებიც შეიძლება გამოყენებულ იქნას სისტემაში ან ქსელში არაავტორიზებული წვდომის მოსაპოვებლად. სოციალური ინჟინერიის შეტევების მაგალითები მოიცავს ფიშინგს, პრეტექსტირებას და სატყუარას.

**კონსენსუსი/სოციალური მტკიცებულება**

კონსესუსის ან სოციალური მტკიცებულების პრინციპი გულისხმობს იმას რომ გარკვეული ქცევის ინსტრუქცია არ არსებობს, აქედან გამომდინარე ბევრი ადამიანი ისე იქცევა, როგორც ფიქრობს რომ ადამიანების უმეტესობა მოიქცეოდნენ. სოციალური ინჟინერიის თავდასხმას შეუძლია გამოიყენოს ეს ინსტინქტი ან დაარწმუნოს სამიზნე, რომ მოთხოვნაზე უარის თქმა უცნაური იქნებოდა, ან მოიქცეს თავაზიანად შენობაში შესვლამდე, სანამ ვინმე მათ კარს უჭერს. როგორც კიდევ ერთი მაგალითი, თავდამსხმელს შეუძლია მოატყუოს მომხმარებელი და დააჯეროს, რომ მავნე ვებსაიტი რეალურად ლეგიტიმურია მრავალი ყალბი მიმოხილვისა და ჩვენებების გამოქვეყნებით, რომლებიც აქებენ საიტს. მომხმარებელი ჩათვლის რომ მრავალმა სხვადასხვა ადამიანმა შეაფასა ეს საიტი და ეჭვის საფუძველი არ არსებობს, შესაბამისად ენდობა მას.

სტატიკური და დინამიური მალვეარის ანალიზები:

**სტატიკური ანალიზი**

როდესაც მავნე პროგრამა ანალიზდება შესრულების გარეშე, მას სტატიკური ანალიზი ეწოდება. ამ შემთხვევაში, PE ფაილის სხვადასხვა თვისებები გაანალიზებულია მისი გაშვების გარეშე. ანალოგიურად, მავნე დოკუმენტის შემთხვევაში, დოკუმენტის თვისებების შესწავლა მისი ანალიზის გარეშე ჩაითვლება სტატიკური ანალიზად. სტატიკური ანალიზის მაგალითები მოიცავს მავნე პროგრამაში სტრიქონების შემოწმებას, PE სათაურის შემოწმებას სხვადასხვა განყოფილებებთან დაკავშირებული ინფორმაციისთვის, ან კოდის დათვალიერებას დემონტაჟის გამოყენებით. მავნე პროგრამა ხშირად იყენებს ტექნიკას სტატიკური ანალიზის თავიდან ასაცილებლად. ზოგიერთი ეს ტექნიკა იყენებს დაბნელებას, შეფუთვას ან მისი თვისებების დამალვის სხვა საშუალებებს. ამ ტექნიკის გვერდის ავლით, ჩვენ ხშირად ვიყენებთ დინამიურ ანალიზს.

**დინამიური ანალიზი:**

სტატიკურმა ანალიზმა შეიძლება მოგვაწოდოს გადამწყვეტი ინფორმაცია მავნე პროგრამების შესახებ, მაგრამ ზოგჯერ ეს საკმარისი არ არის. შეიძლება დაგჭირდეთ მავნე პროგრამის გაშვება კონტროლირებად გარემოში, რათა დავაკვირდეთ, რას აკეთებს ის ამ შემთხვევებში. მავნე პროგრამას ხშირად შეუძლია დამალოს თავისი თვისებები სტატიკური ანალიზის ჩაშლის მიზნით. თუმცა, უმეტეს შემთხვევაში, **დინამიური ანალიზი** შეიძლება იყოს ნაყოფიერი. დინამიური ანალიზის ტექნიკა მოიცავს მავნე პროგრამის გაშვებას VM-ში, ან ხელით, მავნე პროგრამის აქტივობის მონიტორინგისთვის დაინსტალირებული ხელსაწყოებით ან ქვიშის ყუთების სახით, რომლებიც ასრულებენ ამ ამოცანას ავტომატურად. უპირატესობა აქ არის ის, რომ რადგან ჩვენ ვაკონტროლებთ გარემოს, შეგვიძლია მისი კონფიგურაცია ისე, რომ თავიდან ავიცილოთ ხმაური, როგორიცაა ლეგიტიმური მომხმარებლის აქტივობა ან Windows სერვისები. ამრიგად, ყველაფერი, რასაც ჩვენ ვაკვირდებით ასეთ გარემოში, მიუთითებს მავნე პროგრამის აქტივობაზე, რაც აადვილებს იმის დადგენას, თუ რა გააკეთა მავნე პროგრამამ ამ სცენარში.

**Firewall** არის მოწყობილობა,რომლის დახმარებითაც ხორციელდება ორგანიზაციის ქსელური ტრეფიკის(network traffick) მონიტორინგი, წინასწარ განსაზღვრული წესებისშესაბამისად. ის შეიძლება იყოს როგორც აპარატურული, ისე პროგრამული სახის. Firewall-ის გამოყენებით შესაძლოა გავაკონტროლოთ ქსელური პროტოკოლები, პორტები, განვსაზღვროთ თუ რომელ IP მისამართებზე იყოს წვდომა დაშვებული და რომელზე არა.

Firewall როგორცწესი, მოთავსებულია კორპორატიული ქსელის ე.წ DMZ(DeMilitarized Zone)-ში, რაც, მარტივად რომ ვთქვათ, არის ქსელის ნაწილი, სადაცგანთავსებულია ყველაის სერვისი, რომელსაც სჭირდება ინტერნეტზე წვდომა სამუშაოდ(მაგ VOIP, Web, Mail სერვერებიდა ა.შ). Firewall-ები, როგორცწესი, მუშაობენ OSI მოდელის მესამე დამეოთხე დონეებზე, გამონაკლისია მხოლოდ WAF, რომელიცმუშაობს მე-7 დონეზე.

**Whitelisting** არის მონიტორინგის მეთოდი, რომლისდროსაც ორგანიზაცია განსაზღვრავს კონკრეტული სახის ვებ-რესურსებს(მაგ.ვებ-გვერდებს)რომელზე წვდომაც არის დასაშვები, ხოლო ყველასხვა დანარჩენ ვებ-რესურსზე წვდომა იზღუდება.

**Blacklisting** არის მონიტორინგის მეთოდი, რომლისდროსაცორგანიზაციის მიერ განისაზღვრება არასასურველი ვებ-რესურესები, რომლებზეწვდომაცარისდაუშვებელი(მაგ.ვებ-გვერდები), ხოლო ყველასხვა დანარჩენ ვებ-რესურსზე წვდომა ჩვეულებრივღიაა. ასეთი მიდგომა საშუალებას გვაძლევს სწრაფად და მარტივად დავბლოკოთ არასასურველი ვებ-რესურსები.

**Intrusion Detection System(IDS)** - არის სისტემა, რომელსაცშეუძლია აღმოაჩინოს ქსელში ან ჰოსტ-კომპიუტერზე არაავტორიზებული შემოსვლადა ამის შესახებ მოგვცეს გაფრთხილება, რომელსაცშემდგომდაამუშავებს SOC ჯგუფი.

არსებობს ორი ტიპის IDS: **Host-Based IDS (HIDS)**- ახდენს მხოლოდ იმ სისტემის(იქნება ეს კომპიუტერი თუ სერვერი) დაცვას, რომელზეც არის დაინსტალირებული.

**Network-Based IDS (NIDS)-** ახდენს მთლიანი ქსელის მონიტორინგს და შეტყობინებას გვაძლევს არაავტორიზებული ქმედების განხორციელების შემთხვევაში. არაავტორიზებული წვდომის ან ქმედების აღმოჩენა ხორციელდება სამი მეთოდით:

**Signature Detection** - არაავტორიზებული წვდომის ან ქმედების აღმოჩენა ხდება მათი მოქმედების სპეციფიკიდან გამომდინარე, ანუ პროგრამას აქვს გაწერილი ყველა ის მავნე აქტორი, რაც დროის მოცემულ მომენტშია ცნობილი და მათი გამოყენებით ის „ცნობს“ მათ და გვაძლევს გაფრთხილებას.

**Anomaly Detection**- პროგრამა „სწავლობს“ თუ რა პროცესები, მომხმარებლები, სისტემებიდა ა.შ გვაქვს ქსელში ან ჰოსტზე ჩვეულებრივდა ამას იღებს ნორმად. თუ მიღებულ ნორმაში დაფიქსირდაცვლილება, ვთქვათ, ქსელშიდაემატა ახალი ჰოსტ-კომპიუტერი, პროგრამა ამას აღიქვამს როგორც ანომალიას და მოგვცემს გაფრთხილებას.

**Hybrid Detection** - პროგრამა იყენებს როგორც Signature, ისე Anomaly Detection-ს ერთდროულად.

გადაცემის კონტროლის პროტოკოლი (**TCP**) არის საკომუნიკაციო სტანდარტი, რომელიც საშუალებას აძლევს აპლიკაციურ პროგრამებს და გამოთვლით მოწყობილობებს გაცვალონ შეტყობინებები ქსელში. იგი შექმნილია იმისთვის, რომ გაგზავნოს პაკეტები ინტერნეტში და უზრუნველყოს მონაცემთა და შეტყობინებების წარმატებული მიწოდება ქსელებში.

მომხმარებლის მონაცემთა გრამის პროტოკოლი (**UDP**) არის საკომუნიკაციო პროტოკოლი, რომელიც ძირითადად გამოიყენება ინტერნეტში აპლიკაციებს შორის დაბალი შეყოვნების და დანაკარგის შემწყნარებლური კავშირების დასამყარებლად. UDP აჩქარებს გადაცემას მიმღები მხარის მიერ შეთანხმების გაფორმებამდე მონაცემთა გადაცემის ჩართვით.

**HTTP** (ჰიპერტექსტის გადაცემის პროტოკოლი) არის ფაილების ინტერნეტში გადაცემის წესების ნაკრები - როგორიცაა ტექსტი, სურათები, ხმა, ვიდეო და სხვა მულტიმედიური ფაილები. როგორც კი მომხმარებელი ხსნის თავის ბრაუზერს, ის ირიბად იყენებს HTTP-ს.

**HTTPS** (ჰიპერტექსტის გადაცემის პროტოკოლის უსაფრთხო)  არის HTTP-ის უსაფრთხო ვერსია, რომელიც არის პირველადი პროტოკოლი, რომელიც გამოიყენება მონაცემთა გასაგზავნად ვებ ბრაუზერსა და ვებსაიტს შორი