საბოლოო მოწყობილობების სისუსტეები

საბოლოო მოწყობილობა არის, მოწყობილობა ან გარკვეული ლოკაცია ქსელში სადაც კომუნიკაცია იწყება ან მთავრდება, ეს შეიძლება იყოს ფიზიკური დივაისი, როგორებიცაა კომპიუტერი, ლეპტოპი სერვერი, ან ვირტუალური ერთეული მაგალითად ვირტუალური მანქანა არ ქსელის სერვისი. ენდფოინთები ქსელის საჭირო კომპონენტებია, რადგან ისინი უზრუნველყოფენ კომუნიკაციას იუზერებს, აპლიკაციებს ან დეივაისებს შორის.მათ შეუძლიათ გაგზავნონ ან მიიღონ დატა, მიიღონ წვდომა ქსელურ რესურსებზე ან ირუთიერთქმედონ სხვა ენდფოინთებთან ან სერვისებთან.

რაც შეეხება სისუსტეებს, ენდფოით დივაისებს როგორორებიცაა, კომპიუტერი, ლეპტოპი, სმარტფონი და ტაბლეტი შეიძლება გააჩნდეს სისუსტეები მათ დაცვის კონტროლზე, რაც გამოიწვევს მათ დაუცველობას შეტევის მიმართ. მათ შორის გაცრცელებული სისუსტეებია:

ვადაგასული სოფთვეარი და ოპერაციული სისტემა: ენდფოინთებს ვადაგასული სოფთვეართით ან ოპერაციული სისტემით შეიძლება ჰქონდეს ეთექერებისთვის ცნობილი დაუცველობები რომლებსაც შემდგომ ისინი გამოიყენებენ.

სუსტი პაროლები: ენდფოინთები სუსტი ან მარტივად გამოსაცნობი პაროლებით შეიძლება გახდეს ბრიუთფორს შეტევის ან პაროლის გამოცნობის შეტევის მსხვერპლი.

დაცვის სოფთვეარის არარსებობა: ედნფოინთები ანტივირუსის ან ანტიმალვეარის ან სხვა რაიმე დაცვის გარეშე, ხდება დაუცველი და მარტივად ხელმისაწვდომი ათაქერებისთვის.

არასწორად დაკონფიგურირებული დაცვის კონტროლის მექანიზმები როგორიცაა მაგალითად ფაირვოლი შეიძლება ენდფოინთის დაუცველობის მთავარი მიზეზი გახდეს.

არადაცული დისტანციური წვდომა როგორიცაა სუსტი პაროლები ან დაუშიფრავი კავშირი ასევე შესაძლებელია დაუცველობის მთავარი მიზეზი გახდეს

სოციალური ინჟინერიის შეტევები ენდფოინთის კიდევ ერთი სისუსტეა, როგორიცაა ფიშინი ან სფეარ ფიშინგი

ფიზიკური ქურდობა ან დაკარგვა: ენდფოინთები შეიძლება მოიპარონ ან დაიკარგოს რაც გამოიწვევს სენსიტიური ინფორმაციის გაჟონვას ან ათაქერებს უფლებას მისცემს წვდომა მოიპოვონ შიდა სისტემაზე.

ენდფოინთების კიდევ ერთი სისუსტე შეიძლება იყოს მომხარებლის შეცდომა რომელიც მგალითად გადმოწერს რაიმე მალვეარს.

ორგანიზაციებისთვის მნიშვენლოვანია რომ რეგულარულად აკონტროლოს თავიანთი ენდფოინთების დაცულობა რომ მინიმალურ რისკებამდე დაიყვანონ რაიმე ჩავარდნა დაცვაში.ეს შეიძლება იყოს, ძლიერი პაროლები,

სოფთევარის და სისტემის რეგულარული აპდეითი, გამართული დაცვის სისტემა და ა.შ

წვდომის კონტროლის მოდელები

წვდომის კონტროლი მოიცავს მართვისა და შეზღუდვის პროცესს თუ ვის შეიძლება ჰქონდეს წვდომა ფიზიკურ ან ციფრულ რესურსებზე. ეს არის დაცვის მექნაიზმი რომელიც გამოიყენება რომ დავრწმუნდეთ რომ მხოლოდ ავტორიზებულ პირებს ენიჭებათ წვდომა სპეციფიკურ არეაზე ან რესურსებზე.

წვდომის კონტროლის მოდელი ბევრ სხვადასხვა ტიპს შეიცავს მათ შორის გამორჩეულია დისკრეციული, სავალდებულო და როლზე დაფუძვნებული წვდომის კონტროლები.

დისკრეციული წვდომის კონტროლი ანუ DAC რაც გულისხმობს რომ, მფლობელს აქვს სრული წვდომა თავის შექმნილ რესურსზე, მას შეუძლია შეცვალოს რესურსზე წვდომის კონტროლის სია, მიანიჭოს სხვას ან ჩამოართვას. დისკრეციული წვდომის კონტროლი ყველაზე მოქნილი ტიპია კონტროლებს შორის და ფართოდაა დანერგილი. ეს წვდომის კონტროლი დეფოლთად გამოიყენება იუნიხ/ლინუქსში და მაიქროსოფტ ვინდოუში. ის რომ ეს წვდომის კონტროლი ყველაზე გავრცელებულია ასევე ყველაზე სუსტიცაა.

როლზე დაფუძვნებული წვდომის კონტროლი განავცობს დისკრეციულ წვდომის კონტროლს. როგორც სიტყვა გვეუბნება ეს წვდომის კონტროლი დაფუძნებულია როლებზე. მაგალითად ფინანსური დეპარტამენტის უფროსს რომელსაც აქვს წვდომა ფინანსურ რესურსებთან არ შეუძლია წვდომა ჰქონდეს სხვა დეპარტამენტის რესურსებთან. ასევე არსებობს იერარქიაც უფრო მაღალი წოდების პირს შეიძლება ჰქონდეს წვდომა და უფრო დაბალს არა.

სავალდებულო წვდომის კონტოლი წვდომის უფლებას დაცვის ლეიბლების მიხედვით რომელიც მინიჭებულია რესურსებზე მისი სენსიტიურობის მიხედვით.

კიბერუსაფრთხოების როლები

CISO, ან ინფორმაციული უსაფრთხოების მთავარი ოფიცერი, არის უმაღლესი დონის აღმასრულებელი, რომელიც აკონტროლებს ორგანიზაციის ინფორმაციას, კიბერ და ტექნოლოგიურ უსაფრთხოებას. CISO-ს პასუხისმგებლობა მოიცავს უსაფრთხოების პოლიტიკის შემუშავებას, განხორციელებას და აღსრულებას კრიტიკული მონაცემების დასაცავად.

კიბერ ინციდენტებზე მრეაგირებელი: ეს როლი იძიებს, აანალიზებს და რეაგირებს კიბერ ინციდენტებზე ქსელის გარემოში.

შესაბამისობის ოფიცერი არის პროფესიონალი, რომელიც აფასებს შეესაბამება თუ არა ორგანიზაციის პოლიტიკა და პროცედურები კიბერუსაფრთხოებასთან დაკავშირებულ მოქმედ კანონებსა და რეგულაციებს, რითაც გაზრდის მის დაცვას კიბერშეტევებისგან.

კიბერ დაზვერვის ანალიტიკოსები, ასევე ცნობილი როგორც „კიბერ საფრთხეების ანალიტიკოსები“, არიან ინფორმაციული უსაფრთხოების პროფესიონალები, რომლებიც იყენებენ თავიანთ უნარებსა და ცოდნას საფრთხის შესახებ მონაცემების შესაგროვებლად და გასაანალიზებლად, რათა შექმნან დაზვერვა ანგარიშების სახით და გაუზიარონ შესაბამის დეპარტამენტს.

კიბერუსაფრთხოების არქიტექტორი პასუხისმგებელია ორგანიზაციის IT ქსელში უსაფრთხოების სისტემების დიზაინზე, შექმნასა და შენარჩუნებაზე, მათ შორის კომპიუტერული სისტემებისა და მონაცემების ჩათვლით.

კიბერუსაფრთხოების აუდიტი მოიცავს ბიზნესის IT ინფრასტრუქტურის ყოვლისმომცველ ანალიზს და მიმოხილვას. ის აღმოაჩენს დაუცველობას და საფრთხეებს, აჩვენებს სუსტ კავშირებს და მაღალი რისკის პრაქტიკას.

კიბერუსაფრთხოების პროფესორი ან ინსტრუქტორი პასუხისმგებელია ეფექტური სწავლების სტრატეგიების შემუშავებაზე და გამოყენებაზე კიბერუსაფრთხოების თემაზე სტუდენტების შესაძლებლობების განვითარება.

კიბერუსაფრთხოების განმახორციელებელი პასუხისმგებელია ორგანიზაციის ფარგლებში კიბერუსაფრთხოების ზომების, პოლიტიკისა და ტექნოლოგიების განხორციელებაზე. ისინი უზრუნველყოფენ უსაფრთხოების ზომების ეფექტურად ინტეგრირებას ორგანიზაციის ინფრასტრუქტურასა და სისტემებში, კიბერ საფრთხეებისგან დასაცავად.

შეღწევადობის ტესტერები, ან მოკლედ კალმის ტესტერები, ახორციელებენ იმიტირებულ კიბერშეტევებს კომპანიის კომპიუტერულ სისტემებსა და ქსელებზე.

სოციალური ინჟინერია

სოციალური ინჟინერია არის ტერმინი, რომელიც გამოიყენება ნებისმიერი კიბერშეტევის აღსაწერად, სადაც სამიზნე ადამიანია (და არა კომპიუტერი); ამ მიზეზით, მას ხანდახან მოიხსენიებენ, როგორც "ხალხის ჰაკერს". მაგალითად, თუ თავდამსხმელს სურს მიიღოს მსხვერპლის პაროლი, მას შეუძლია სცადოს პაროლის გამოცნობა ან უხეში ძალისხმევით — ან შეიძლება უბრალოდ გკითხოთ.

მიუხედავად იმისა, რომ ზემოთ მოყვანილი მაგალითი შედარებით მარტივია, სოციალური ინჟინერიის თავდასხმები შეიძლება გახდეს ძალიან რთული და ხშირად მოჰყვეს თავდამსხმელის მნიშვნელოვან კონტროლს სამიზნის ცხოვრებაზე - როგორც ონლაინ, ასევე ოფლაინზე. სოციალური ინჟინერიის შეტევები ხშირად მრავალფენიანია და ესკალაცია ხდება თოვლის ბურთის ეფექტის გამო. მაგალითად, თავდამსხმელმა შეიძლება დაიწყოს მცირე რაოდენობის საჯაროდ ხელმისაწვდომი ინფორმაციის მოპოვებით მსხვერპლის სოციალურ მედიაში ყოფნიდან, რომელიც შემდეგ მათ შეუძლიათ გამოიყენონ დამატებითი ინფორმაციის მისაღებად, მაგალითად, თქვენი ტელეფონის ან ფართოზოლოვანი პროვაიდერისგან. მეორე ეტაპიდან მიღებული ინფორმაცია შეიძლება გამოყენებულ იქნას უფრო სასარგებლო ინფორმაციის მოსაპოვებლად, შემდეგ კი ეტაპობრივად გადაიზარდოს მსხვერპლის საბანკო ანგარიშზე.

**ციფრული სერთიფიკატები -** ციფრული სერთიფიკატი არის ციფრული ფაილი, რომელიც ადასტურებს ინდივიდის, ორგანიზაციის ან ვებსაიტის იდენტურობას. ის შეიცავს ინფორმაციას, როგორიცაა მფლობელის სახელი, საჯარო გასაღები და სხვა საიდენტიფიკაციო ინფორმაცია, ასევე ციფრული ხელმოწერა სანდო მესამე მხარისგან, რომელიც ცნობილია როგორც სერტიფიკატის ავტორიტეტი.

**ბლოკური და ნაკადური შიფრები -** ნაკადური შიფრაციის დროს დატას თითოეული ბაიტი ან ბიტი იშიფრება ერთდროულად, ამ ტიპის შიფრაცია კარგია იმ ტიპის კომუნიკაციის დროს როდესაც დატას ან მესიჯის სრული სიგრძე არ არის ცნობილი.

რაც შეეხება ბლოკურ შფრაცას დატა იყოფა ტოლი სიგრძის ბლოკებად

ძირითადად 128ბიტის ტოლია, თუ ზუსტად არ იყოფა დატა მაშინ მას ემატება საჭირო ბიტების რაოდენობა რაიმე სტრინგით ალგორითმის გათვალისწინებით.

**კრიპტოგრაფიული გასაღები -** კრიპტოგრაფიული გასაღები, არის ინფორმაციის ნაწილი, რომელიც გამოიყენება კრიპტოგრაფიულ ალგორითმებში მონაცემთა დაშიფვრის ან გაშიფვრის მიზნით. ეს არსებითად არის ბიტების ან სიმბოლოების სტრიქონი, რომელიც ემსახურება როგორც პარამეტრს, რათა აკონტროლოს ჩვეულებრივი ტექსტის ტრანსფორმაცია შიფრულ ტექსტად ან პირიქით. კრიპტო გასაღებები აუცილებელია კრიპტოგრაფიული სისტემების მონაცემების კონფიდენციალურობის, მთლიანობისა და ავთენტურობის უზრუნველსაყოფად.

**ციფრული ხელმოწერა -** ციფრული ხელმოწერები არის ფაილების ავთენტურობის დასამტკიცებლად, იმის დასამტკიცებლად, თუ ვინ შექმნა ან შეცვალა ისინი. ასიმეტრიული კრიპტოგრაფიის გამოყენებით, თქვენ აწარმოებთ ხელმოწერას თქვენი პირადი გასაღებით და მისი გადამოწმება შესაძლებელია თქვენი საჯარო გასაღების გამოყენებით. ვინაიდან მხოლოდ თქვენ უნდა გქონდეთ წვდომა თქვენს პირად გასაღებზე, ეს ადასტურებს, რომ თქვენ მოაწერეთ ხელი ფაილს.

**ქეში -** თითოეულ მოწყობილობას ქსელში აქვს ჩანაწერი ინფორმაციის შესანახად, რომელსაც ქეში ეწოდება.  ARP პროტოკოლის კონტექსტში, ეს ქეში ინახავს ქსელში არსებული სხვა მოწყობილობების იდენტიფიკატორებს.

**Salting -** Salting არის ტექნიკა, რომელიც გამოიყენება კრიპტოგრაფიაში პაროლის შენახვისა და კრიპტოგრაფიული ჰეშის ფუნქციების უსაფრთხოების გასაძლიერებლად. იგი გულისხმობს შემთხვევითი ან უნიკალური მნიშვნელობის დამატებას, რომელიც ცნობილია როგორც salt, შეყვანისთვის, სანამ ის ჰეშირდება ან დაშიფრული იქნება. დანამატი, როგორც წესი, არის ბიტების ან სიმბოლოების შემთხვევითი სტრიქონი, რომელიც გენერირებულია თითოეული მომხმარებლისთვის ან მონაცემთა შეყვანისთვის.

**სიმეტრიული და ასიმეტრიული დაშიფვრა -** სიმეტრიული დაშიფვრა იყენებს ერთ სექრეთ ქის როგოც დაშიფვრისთვის ასევე გაშიფვრისთვის. სიმეტრიული დაშიფვრა ძალიან სწრაფია და გამოიყენება დიდი მოცულობის მონაცემების დასაშფვრად.

რაც შეეხება ასიმეტრიულ დაშფვრას, ის იყენებს ორ სხვადასხვა ქის დასაშფრად და გასაშიფრად ერთი გასაღები არის საჯარო და შესაძლებელია ყველას გავუზიაროთ ხოლო მეროე გასაღები არის დაცული და მხოლოდ მფლობელმა იცის.საჯარო გასაღებით დაშიფვრული მონაცემები მხოლოდ ამ დაცული გასაღებით შეიძლება გაიშიფროს და პირიქით.

**ცისარტყელას ცხრილი -** ცისარტყელას ცხრილი არის წინასწარ გამოთვლილი ცხრილი, რომელიც შეიცავს უამრავ პოტენციურ უბრალო ტექსტს ჰეშის ფუნქციებისთვის. ცისარტყელას ცხრილის დანიშნულებაა დააჩქაროს ჰეშირებული მნიშვნელობების თავდაპირველი ტექსტის ფორმაში დაბრუნება, პაროლების ან სხვა ჰეშირებული მონაცემების ეფექტურად გატეხვა.

**იდენთიფიკაცია ავთენტიპიკაცია ავტორიზაცია** - იდენთიფიკაცია: ანგარიშის ან პირადობის მოწმობის შექმნა, რომელიც ცალსახად

წარმოადგენს მომხმარებელს, მოწყობილობას ან პროცესს ქსელში.

ავთენტიფიკაცია: იმის დამტკიცება, რომ საგანი არის ის ვინც ან რაც აცხადებს რომ ცდილობს რესურსზე წვდომას.

ავტორიზაცია: მოიცავს, თუ რა უფლებები უნდა ჰქონდეთ სუბიექტებს თითოეულ

რესურსზე და ამ უფლებების აღსრულებას.

• იდენტიფიკაცია - დარწმუნდით, რომ მომხმარებლები არიან ლეგიტიმური. მაგალითად, შეიძლება დაგჭირდეთ დარწმუნდეთ, რომ ბილინგისა და მიწოდების მისამართები ემთხვევა და რომ ისინი არ ცდილობენ გამოიყენონ თაღლითური გადახდის მეთოდები.

• ავთენტიფიკაცია - დარწმუნდით, რომ კლიენტებს აქვთ უნიკალური ანგარიშები და რომ მხოლოდ მათ შეუძლიათ თავიანთი შეკვეთების და ბილინგის ინფორმაციის მართვა.

• ავტორიზაცია - წესები, რომლებიც უზრუნველყოფენ კლიენტებს შეკვეთების განთავსება მხოლოდ მაშინ, როდესაც მათ აქვთ გადახდის მოქმედი მექანიზმები. თქვენ შეიძლება აწარმოოთ ლოიალობის სქემები ან აქციები, რომლებიც უფლებას აძლევს გარკვეულ მომხმარებელს ნახონ უნიკალური შეთავაზებები ან კონტენტი.

**ინფორმაციულობა მთლიანობა განსაზღვრა -** ინფორმაციის უსაფრთხოება (ან infosec) მოიცავს მონაცემთა რესურსების დაცვას არაავტორიზებული წვდომისგან, თავდასხმისგან, ქურდობისგან ან დაზიანებისგან. მონაცემები შეიძლება იყოს დაუცველი მათი შენახვის, გადაცემის ან პროცესში. ინფორმაციული უსაფრთხოების სამი ძირითადი პრინციპი, რომელსაც მოიხსენიებენ როგორც CIA (confidentiality integrity availability) ტრიადად, არის:

კონფიდენციალურობა ნიშნავს, რომ გარკვეული ინფორმაცია უნდა იყოს ცნობილი მხოლოდ გარკვეული ადამიანებისთვის.

მთლიანობა ნიშნავს, რომ მონაცემები ინახება და გადაცემულია ისე, როგორც დანიშნულებისამებრ, და რომ ნებისმიერი ცვლილება ავტორიზებულია.

ხელმისაწვდომობა ნიშნავს, რომ ინფორმაცია ხელმისაწვდომია მათთვის, ვინც უფლებამოსილია ნახოს ან შეცვალოს იგი.

**მალვეარი -** მალვეარი არის მავნე პროგრამა რომელსაც დიდი ზიანის გამოწვევა შეუძლია როგორც კომპიუტერული სისტემისთვის ისევე მომხარმებლისთივს. მალვეარის ბევრი ტიპი არსებობს ესენია : ვირუსები, ტროას ცხენები, ჭიები ანუ ვორმები, რენსომვეარი, ბექდორი და რუთკიტი.

**ინციდენტზე რეაგირება -** ინციდენტებზე რეაგირების პოლიტიკა ადგენს რესურსებს, პროცესებსა და მითითებებს უსაფრთხოების ინციდენტების მოსაგვარებლად. ინციდენტების მართვა სასიცოცხლოდ მნიშვნელოვანია რისკის შესამცირებლად. ის მოიცავს მომზადებას, იდენტიფიცირებას, შეკავებას, აღმოფხვრას, აღდგენას, გაკვეთილის სწავლას.

**რისკი -** რისკი ეხება სენსიტიურ ინფორმაციაზე, სისტემებსა თუ რესურსებზე დარღვევის, კომპრომისის ან არაავტორიზებული წვდომის პოტენციალს.

რისკის იდენტიფიკაცია არის პოტენციური რისკების ან საფრთხეების იდენტიფიცირებისა და გაგების პროცესი, რომელთა წინაშეც შეიძლება აღმოჩნდეს ორგანიზაცია. ის გულისხმობს სხვადასხვა ფაქტორების სისტემატურ იდენტიფიცირებას, დოკუმენტირებას და ანალიზს, რამაც შეიძლება გამოიწვიოს უსაფრთხოების ინციდენტები ან დაუცველობა. რისკის იდენტიფიკაციის მიზანია ორგანიზაციის პოტენციური რისკების გააზრება, რათა შეიმუშაოს რისკის მართვის ეფექტური სტრატეგიები და კონტროლი.

მისიის არსებითი ფუნქციების იდენტიფიცირება

მოწყვლადობის იდენტიფიცირება

საფრთხეების იდენტიფიცირება

გაანალიზეთ ბიზნესის გავლენა

რისკზე რეაგირების იდენტიფიცირება

**ფაირვოლი და ანტივირუსი:** Firewall არის მოწყობილობა ქსელში, რომელიც პასუხისმგებელია იმის განსაზღვრაზე, თუ რა ტრაფიკს შეუძლია შესვლა და გასვლა. იფიქრეთ firewall- ზე, როგორც ქსელის საზღვრის უსაფრთხოებაზე. ადმინისტრატორს შეუძლია დააკონფიგურიროს firewall, რათა დაუშვას ან უარყოს ტრაფიკი ქსელში შესვლის ან გასვლისგან, მრავალი ფაქტორის საფუძველზე, როგორიცაა:

საიდან მოდის ტრაფიქი

სად მიდის ტრაფიქი

რომელი პორტისთვისაა ტრაფიქი

რა პროტოკოლს იყენებს ტრაფიკი

ანტივირუსული (AV) პროგრამა არის უსაფრთხოების დამატებითი ფენა, რომელიც მიზნად ისახავს აღმოაჩინოს და თავიდან აიცილოს მავნე ფაილების გაშვება და გავრცელება სამიზნე ოპერაციულ სისტემაში.