კიბერსაფრთხეების სიმულაციური სავარჯიშოების პერიოდული განხორციელების საჭიროება უნივერსიტეტის პერსონალისთვის

ავთანდილ ბიჩნიგაური
ასოცირებული პროფესორი, საქართველოს ტექნიკური უნივერსიტეტი
bichnigauri_av@gtu.ge
დავით ბიჩნიგაური
ასოცირებული პროფესორი, საქართველოს ტექნიკური უნივერსიტეტი
davit.bichnigauri@gmail.com
ლუკა შონია
ასისტენტ პროფესორი, საქართველოს ტექნიკური უნივერსიტეტი
shonia@gtu.ge
https://doi.org/10.61950/giu.4.2026.12142

აბსტრაქტი

კიბერ და ინფორმაციული უსაფრთხოების უზრუნველყოფა თანამედროვე უნივერსიტეტებისთვის ერთ-ერთი ყველაზე კრიტიკული გამოწვევაა. უნივერსიტეტები, როგორც ღია აკადემიური გარემოები და საინფორმაციო რესურსებით მდიდარი ცენტრები, განსაკუთრებით დაუცველია კიბერთავდასხმების მიმართ. მოცემულ სტატიაში არგუმენტირებულად წარმოდგენილია, რომ უნივერსიტეტის პერსონალისთვის კიბერსაფრთხეების სიმულაციური სავარჯიშოების პერიოდული განხორციელება არა რეკომენდაცია, არამედ აუცილებელი კომპონენტია ორგანიზაციული კიბერდაცვის შექმნისა და შენარჩუნებისთვის. სტატიაში განხილულია სიმულაციების ძირითადი ტიპები (ფიშინგი, რენსომვეარი, DDoS, ინციდენტებზე რეაგირების მექანიზმები), მათი ტექნიკური უზრუნველყოფის მეთოდოლოგია და მოსალოდნელი შედეგები. ხაზგასმულია, რომ პერიოდულობა საშუალებას აძლევს არა მხოლოდ ცოდნის განახლებას, არამედ უწყვეტი გაუმჯობესების ციკლის (Continuous Improvement Cycle) დანერგვას, რაც საბოლოოდ ამცირებს რისკებს და აძლიერებს უნივერსიტეტის მთლიან უსაფრთხოების მდგომარეობას.

საკვანძო სიტყვები: კიბერუსაფრთხოება, სიმულაციური სავარჯიშოები, ფიშინგი, რენსომვეარი, ინციდენტებზე რეაგირების გეგმა (IRP), სოციალური ინჟინერია, ცნობიერების ამაღლება, უნივერსიტეტის IT-ინფრასტრუქტურა, უწყვეტი გაუმჯობესების ციკლი.

შესავალი

თანამედროვე უმაღლესი განათლების დაწესებულებები წარმოადგენენ რთულ ორგანიზმებს, რომლებიც აერთიანებენ სასწავლო, სამეცნიერო და ადმინისტრაციულ ფუნქციებს. მათი ციფრული ეკოსისტემა მოიცავს სტუდენტთა და პერსონალის პერსონალურ მონაცემთა ბაზებს, საავტორო უფლებებით დაცულ სამეცნიერო კვლევებს, ფინანსურ დოკუმენტაციას, სასწავლო პროცესის მართვის სისტემებსა და კრიტიკულ ინფრასტრუქტურას. ეს ყველაფერი მათ მიმზიდველ სამიზნედ აქცევს კიბერდამნაშავეებისთვის.

უნივერსიტეტებისთვის დამახასიათებელი ღიაობა, დეცენტრალიზებული IT-ინფრასტრუქტურა და პერსონალისა და სტუდენტების მუდმივი ბრუნვა ქმნის უნიკალურ გამოწვევებს კიბერუსაფრთხოებისთვის. ხშირად, ტექნიკური დაცვის ყველაზე მოწინავე სისტემებიც კი ვერ ანეიტრალებს ადამიანურ ფაქტორს, რომელიც ყველაზე დიდ სისუსტეს წარმოადგენს. სტატისტიკა მიუთითებს, რომ დანაშაულის 80%-ზე მეტში გამოიყენება სოციალური ინჟინერიის მეთოდები, რაც პირდაპირ კავშირშია პერსონალისა და მომხმარებლების ცნობიერების დაბალ დონესთან.

აღნიშნული პრობლემის მოგვარების ერთ-ერთი ყველაზე ეფექტური მეთოდია კიბერსაფრთხეების სიმულაციური სავარჯიშოების პერიოდული განხორციელება. ასეთი სავარჯიშოები არა მხოლოდ ასწავლის პერსონალს როგორ ამოიცნოს საფრთხეები, არამედ ქმნის მუდმივ პრაქტიკულ გამოცდილებას, რაც თეორიული ცოდნისგან განსხვავებით, უფრო მტკიცედ ფიქსირდება. აქტუალურია არა მხოლოდ სავარჯიშოების ჩატარება, არამედ მათი სისტემატურობა და პერიოდულობა, რაც განაპირობებს უწყვეტი გაუმჯობესების პროცესს და ადაპტაციას ახალ საფრთხეებთან.

მეთოდოლოგია (ძირითადი ნაწილი)

კიბერსაფრთხეების სიმულაციური სავარჯიშოების ეფექტური განხორციელებისთვის აუცილებელია სტრუქტურირებული მიდგომა. შემოთავაზებული მეთოდოლოგია მოიცავს შემდეგ ეტაპებს:

1. **რისკების შეფასება და მიზნების განსაზღვრა:**
   პირველ რიგში, აუცილებელია ჩატარდეს უნივერსიტეტის IT-ინფრასტრუქტურისა და მონაცემთა სისტემების სრული აუდიტი. განისაზღვრება ყველაზე კრიტიკული აქტივები (მაგ., სამეცნიერო კვლევების არქივი, ფინანსური ჩანაწერები, პერსონალური მონაცემები) და მათთვის არსებული საფრთხეები. მიზნები შეიძლება იყოს: ფიშინგის მიმართ წინააღმდეგობის გაზრდა 25%-ით 6 თვეში, ინციდენტებზე რეაგირების გეგმის (Incident Response Plan - IRP) ტესტირება, პერსონალისთვის რენსომვეარის საფრთხის გაცნობა და ა.შ.
2. **სამიზნე აუდიტორიების იდენტიფიცირება:**
   აღსანიშნავია, რომ ყველა თანამშრომელი ერთნაირი რისკის ქვეშ არ იმყოფება. აუცილებელია შესაბამისი სამიზნე ჯგუფების განსაზღვრა:
   - **ადმინისტრაციული პერსონალი:** მოქმედებს ფინანსურ და პერსონალურ მონაცემებთან. მათთვის კრიტიკულია BEC (Business Email Compromise) თავდასხმების სიმულაცია.
   - **საკადრო სამსახური:** ხშირი სამიზნეა პრეტენდენტების პერსონალური მონაცემების მოპოვების მიზნით.
   - **პროფესორ-მასწავლებელი და აკადემიური პერსონალი:** ფლობენ მნიშვნელოვან ინტელექტუალურ საკუთრებას და საავტორო ნამუშევრებს. მათთვის რელევანტურია სამეცნიერო შპიონაჟისა და დოქსინგის (doxing) სიმულაციები.

- **IT-დეპარტამენტის თანამშრომლები:** მათთვის სავარჯიშოები უნდა იყოს ტექნიკური - DDoS თავდასხმების პრევენცია, მავნე პროგრამული უზრუნველყოფის ანალიზი, IRP-ის აქტივაცია.

3. **სიმულაციის ტიპის შერჩევა:**
   - **ფიშინგის კამპანიების სიმულაცია:** გამოიყენება სპეციალიზებული პლატფორმები (მაგ., KnowBe4, Proofpoint Security Awareness). შეიქმნება რეალისტური ელ. ფოსტის შაბლონები, რომლებიც იმიტირებენ უნივერსიტეტის ადმინისტრაციის, ბანკის ან პოპულარული სერვისის გზავნილებს. ჰიპერბმულები მიმართული იქნება კონტროლირებად ვებგვერდზე. მონაწილეთა ქმედებები (ელ. წერილის გახსნა, ბმულზე დაწკაპუნება, მონაცემების შეყვანა) დაფიქსირდება სისტემაში.
   - **რენსომვეარ-თავდასხმის სიმულაცია:** გამოიყენება უვნებელი ფაილები, რომლებიც იმიტირებენ რენსომვეარის მოქმედებას (მაგ., ფაილის დაშიფვრის იმიტაცია და აღდგენის ინსტრუქციის ჩვენება). ეს ეხმარება პერსონალს ამოიცნოს თავდასხმის ნიშნები და იცოდეს რა უნდა გააკეთოს (გათიშოს კომპიუტერი ქსელიდან, დაუკავშირდეს IT-სამსახურს და ა.შ.).
   - **ინციდენტებზე რეაგირების დრილები (Tabletop Exercises):** ეს არის სიტუაციური თამაშები, რომლებშიც მონაწილეები (როგორც წესი, მენეჯმენტი და IT-სპეციალისტები) ერთობლივად განიხილავენ და აგვარებენ სცენარის მიხედვით შექმნილ კიბერ-ინციდენტს. მაგ., „თქვენმა უნივერსიტეტმა სისტემაში აღმოაჩინა დაშიფრული ფაილი გამოსასყიდის მოთხოვნით. როგორ იმოქმედებთ? ვინ უნდა ჩართოთ? როგორ მოახდენთ სტუდენტების და საზოგადოების ინფორმირებას?“.
   - **DDoS-თავდასხმების სიმულაცია:** ტარდება IT-დეპარტამენტის მიერ კონტროლირებად პირობებში, ტესტირების სერვერებზე, რათა შემოწმდეს ქსელის გამძლეობა და შემზღუდველი მექანიზმების ეფექტურობა.

4. **განხორციელება და მონიტორინგი:**
   სავარჯიშოები ტარდება წინასწარ განცხადებული ან უცრად (რაც უფრო რეალისტურია). ყველა მონაწილის ქმედება ყურდება და ფიქსირდება ანალიზისთვის.

5. **ანალიზი და უკუკავშირი:**
   სავარჯიშოს დასრულების შემდეგ ტარდება მონაცემთა ანალიზი: დაწკაპუნების სიხშირე, მონაცემების შეყვანის პროცენტული მაჩვენებელი, რეაგირების დრო. თითოეულ მონაწილეზე დგინდება ინდივიდუალური ანალიტიკა და მომზადდება შესაბამისი რეკომენდაციები თუ რას დააწკაპუნეს, რატომ იყო ეს საფრთხე, როგორ უნდა ამოიცნონ მსგავსი შემთხვევა მომავალში. იმ თანამშრომლებს, რომლებიც „ჩაიჭრნენ“ სიმულაციის პროცესში, ეძლევათ დამატებითი ტრენინგების გავლის ვალდებულება.

მსჯელობა

კიბერსაფრთხეების სიმულაციური სავარჯიშოების პერიოდულობა არის კრიტიკული ფაქტორი, რომელიც განაპირობებს მათ გრძელვადიან ეფექტს. ერთჯერადი ტრენინგი, თუნდაც ძალიან ინტენსიური, არ გამოიმუშავებს მდგრად შედეგებს. ამის მიზეზები შემდეგია:

1. **ადამიანური ფსიქოლოგია და ცნობიერების შენარჩუნება:** ადამიანებს თანდათანობით ავიწყდებათ ის, რასაც არ იყენებენ, შესაბამისად, კიბერსაფრთხეების ცოდნაც არ არის გამონაკლისი. პერიოდული სიმულაციები მუდმივად ახსენებს პერსონალს საფრთხეების არსებობას და ახალ საფრთხეთა მიმართ თავდაცვით მენტალიტეტს ქმნის. ეს არის მუდმივი განახლების პროცესი, რომელიც ხელს უშლის ცოდნის დაძველებას.
2. **კიბერ-სამიზნეების ევოლუცია:** კიბერდამნაშავეები მუდმივად ახდენენ თავიანთი ტაქტიკის, ტექნიკისა და პროცედურების (TTPs) განახლებას. იმ ფიშინგის ტექნიკა, რომელიც ეფექტური იყო ერთი წლის წინ, დღეს შეიძლება მოძველებული იყოს. პერიოდული სიმულაციები საშუალებას აძლევს უნივერსიტეტს მოქნილად რეაგირება მოახდინოს ამ ცვლილებებზე და სავარჯიშოების სცენარებში ჩაატაროს ახალი ტიპის ისეთი თავდასხმები, როგორებიცაა მობილური ტელეფონის მავნე კოდი (mobile malware), ქვიშინგი (QR code phishing - Quishing), გენერაციული ხელოვნური ინტელექტით შექმნილი დახვეწილი ფიშინგი და ა.შ.
3. **უწყვეტი გაუმჯობესების ციკლი (Continuous Improvement Cycle):** სიმულაციები არის არა მხოლოდ სასწავლო ინსტრუმენტი, არამედ დიაგნოსტიკური ინსტრუმენტიც. თითოეული სავარჯიშოს შედეგები იძლევა უნიკალურ მონაცემებს ორგანიზაციის სისუსტეების შესახებ.
    - **პირველი სავარჯიშო (Q1):** გამოავლენს, რომ 40%-მა პერსონალმა დააწკაპუნა ფიშინგის ბმულზე.
    - **სწავლება და ჩარევა:** ტარდება სპეციალური ტრენინგი და ინდივიდუალური კონსულტაციები.
    - **მეორე სავარჯიშო (Q3):** მაჩვენებელი ეცემა 15%-მდე.
    - **ანალიზი:** 15% მაინც მაღალია. ანალიზი გვიჩვენებს, რომ ამ ჯგუფს ძირითადად წარმოადგენენ არა-ტექნიკური სპეციალობის თანამშრომლები. შემუშავდება მათთვის განკუთვნილი, უფრო მიზნობრივი და მარტივი სასწავლო მასალა.

    ამგვარად, სავარჯიშოების პერიოდულობა საშუალებას აძლევს ორგანიზაციას არა მხოლოდ გაზომოს პროგრესი, არამედ დახვეწოს თავისი კიბერდაცვის სტრატეგია და რესურსების განაწილება.

4. **ინციდენტებზე რეაგირების კულტურის ჩამოყალიბება:** როდესაც რეალური კიბერ-ინციდენტი ხდება, პანიკა და არეულობა ხშირად უფრო დიდ ზიანს აყენებს, ვიდრე თავად თავდასხმა. პერიოდული სავარჯიშოები და სიმულაციები ქმნიან ე.წ. „კუნთების მეხსიერებას“. პერსონალი იწყებს ავტომატურად ფიქრობს: „ეს ელ. ფოსტა საეჭვოა, აჯობებს გადავამოწმო ორგანიზაციის CISO-სთან (Chief Information Security Officer)“ ან „სისტემა გათიშულია, ეს შეიძლება იყოს DDoS შეტევა, ვიმოქმედებ IRP-ის მიხედვით“. ეს პროაქტიული და კოორდინირებული რეაგირების კულტურა არის უფრო ღირებული, ვიდრე ნებისმიერი ცალკეული ტექნოლოგია.
5. **რისკის შემცირება:** სიმულაციების მთავარი მიზანია ადამიანის გადაქცევა უსაფრთხოების ჯაჭვის ყველაზე ძლიერ რგოლად, მისი ყველაზე სუსტიდან გამოყვანა. პერიოდული ვარჯიში ამცირებს მარტივი შეცდომების (პაროლის გაზიარება,

მგრძნობიარე ინფორმაციის გაჟონვა) ალბათობას და ამცირებს წარმატებული თავდასხმების საერთო რაოდენობას.

შედეგები

კიბერსაფრთხეების სიმულაციური სავარჯიშოების პერიოდული განხორციელების შემდეგ, უნივერსიტეტს შეუძლია მოელოდეს შემდეგ რეალურ და გაზომვად შედეგებს:

- **ფიშინგის წინააღმდეგობის მაჩვენებლის ზრდა:**
  დაწკაპუნების სიხშირის (Click-Through Rate - CTR) შემცირება 40%-დან 10%-ზე დაბლა ექვსთვიანი ინტენსიური პროგრამის შედეგად.
- **ინციდენტების აღმოჩენის დროის შემცირება:**
  როდესაც პერსონალი აქტიურად ამცნობს IT-დეპარტამენტს საეჭვო აქტივობებზე, ინციდენტის გამოვლენა და იზოლაცია მნიშვნელოვნად ჩქარდება. მაგ., რეალური რენსომვეარ-თავდასხმის დროს, პირველი შეტყობინება IT-სამსახურში მიიღება არა დღეების, არამედ საათების განმავლობაში.
- **ინციდენტებზე რეაგირების გეგმის (IRP) ეფექტურობის გაზრდა:**
  სავარჯიშოების შედეგად, IRP გახდება უფრო დახვეწილი და პრაქტიკული. ირკვევა კომუნიკაციის ხარვეზები, განსაზღვრულია პასუხისმგებლობის სფეროები, მოქმედებები ხდება უფრო კოორდინირებული.
- **კიბერდაცვის ხარჯების ოპტიმიზაცია:**
  სავარჯიშოები გვიჩვენებს, თუ სად არის ინვესტიციების ყველაზე დიდი საჭიროება. ფინანსები შეიძლება გადამისამართდეს ყველაზე დაუცველი სეგმენტების დასაცავად, ნაცვლად ყველა პოტენციურ სფეროში რესურსების გაფანტვისა.
- **ორგანიზაციული კულტურის ცვლილება:**
  კიბერუსაფრთხოება იქცევა ყველას საერთო საქმედ, და არა მხოლოდ IT-დეპარტამენტის პასუხისმგებლობად. იქმნება გარემო, სადაც თანამშრომლებს არ ეშინიათ დაშვებული შეცდომის აღიარების და დახმარების მოთხოვნის.

დასკვნა

უნივერსიტეტი, როგორც ცოდნისა და ინოვაციების ცენტრი, არ შეიძლება დარჩეს კიბერსაფრთხეების მიმართ მოუმზადებლად. ტექნოლოგიური გადაწყვეტილებები, როგორიცაა ფაირვოლები, ანტივირუსები და სისტემები გამოვლენისთვის (Intrusion Detection Systems), არის აუცილებელი, მაგრამ არასაკმარისი. ადამიანური კაპიტალი რჩება უკანასკნელ ბარიერად და ამავდროულად, პირველ ხაზის დაცვად.

კიბერსაფრთხეების სიმულაციური სავარჯიშოების პერიოდული განხორციელება წარმოადგენს სტრატეგიულ ინვესტიციას ამ კაპიტალის განვითარებაში. ისინი აერთიანებენ განათლებას, პრაქტიკას და უწყვეტ მონიტორინგს ერთ მოქნილ და ადაპტაციურ ჩარჩოში. ასეთი პროგრამა არა მხოლოდ ამცირებს კონკრეტული კიბერ-რისკების ალბათობას, არამედ ქმნის უფრო მდგრად და კიბერ-გათვითცნობიერებულ ორგანიზაციას.

პერიოდულობა არის გასაღები. ის უზრუნველყოფს, რომ ცოდნა არ გაძველდეს, უნარები არ დაიკარგოს და ორგანიზაცია მუდმივად იყოს მზად ახალი და უფრო დახვეწილი საფრთხეებისთვის. ამიტომ, ყველა უნივერსიტეტმა უნდა შეიტანოს სიმულაციური სავარჯიშოები თავისი წლიური საქმიანობის გეგმის ინტეგრალურ ნაწილად და გამოყოს ამისთვის აუცილებელი რესურსები. ეს არის ღირსეული ინვესტიცია აკადემიური თავისუფლების, კვლევის უსაფრთხოების და მთელი აკადემიური საზოგადოების რეპუტაციის დასაცავად.

გამოყენებული ლიტერატურა

1. ა. ბიჩნიგაური, ი. ქართველიშვილი, ლ. შონია - „ფიშინგისა და მავნე კოდის მქონე ვებგვერდების პრევენციის ეფექტური მექანიზმის მოდელის შემუშავება და რეალიზაცია ვებბრაუზერის გარემოში“, *საქართველოს ტექნიკური უნივერსიტეტის საერთაშორისო სამეცნიერო-პრაქტიკული კონფერენცია „თანამედროვე გამოწვევები და მიღწევები ინფორმაციულ ტექნოლოგიებში - 2023“*
2. ა. ბიჩნიგაური, ი. ქართველიშვილი, ლ. შონია - Unveiling Quishing: The Dark Side of QR Codes in Cyber attacks, *ჟურნალი „თავდაცვა და მეცნიერება“.* ტომ. No. 2 (2023), DOI: https://doi.org/10.61446/ds.2.2023.7412
3. ა. ბიჩნიგაური, ი. ქართველიშვილი, ლ. შონია - Strengthening Cyber Defenses - The Crucial Role of Phishing Simulation in Modern Security Strategies, *ჟურნალი „თავდაცვა და მეცნიერება“.* ტომ. No. 3 (2024), DOI: https://doi.org/10.61446/ds.3.2024.8467
4. ა. ბიჩნიგაური, ო. შონია - „ლოკალურ ქსელში IoT მოწყობილობების აღმოჩენის საშუალებები მათი კიბერუსაფრთხოების უზრუნველსაყოფად“, *სამეცნიერო შრომები. მართვის ავტომატიზებული სისტემები. № 1(32), Vol.1. თბილისი, 2021*
5. ა. ბიჩნიგაური, ო. შონია, თ. კაიშაური - „კიბერსაფრთხეების იდენტიფიცირების მიზნით საეჭვო დომენური დასახელებების გამოვლენა CTL ტექნოლოგიის გამოყენებით“, *საქართველოს ტექნიკური უნივერსიტეტის 100 და იმს ფაკულტეტის 65 წლისთავისადმი მიძღვნილი საერთაშორისო სამეცნიერო-პრაქტიკული კონფერენცია „ინოვაციები და თანამედროვე გამოწვევები - 2022“, თბილისი, 2022*
6. კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლების 2025-2030 წლების სტრატეგია - https://dga.gov.ge/files/mUMPR8s3w59z.pdf
7. ENISA (European Union Agency for Cybersecurity). (2021). *Cybersecurity Education in the EU.*
8. საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ - https://matsne.gov.ge/document/view/1679424?publication=8
9. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
10. NIST Special Publication 800-50. Building an Information Technology Security Awareness and Training Program.
11. SANS Institute. (2023). The Human Element in Cybersecurity: Annual Report.
12. CISA (Cybersecurity and Infrastructure Security Agency). (2023). Security Awareness Training Best Practices.

13. ENISA (European Union Agency for Cybersecurity). (2023). Cybersecurity Culture Guidelines for Organizations.
14. Kovacevic, A., & Veinovic, M. (2022). The Role of Tabletop Exercises in Improving Organizational Cyber Resilience. *Journal of Information Security*.
15. Hadlington, L. (2018). The Human Factor in Cybersecurity: Exploring the Accidental Insider. *Psychology Press*.