BDO კიბერ უსაფრთხოების სერვისი
PHISHING AS A SERVICE
(PhaaS)

კიბერ უსაფრთხოების კურსი დისტანციურად მუშაობის დროს

ბოლო პერიოდში მსოფლიოში მკვეთრად გაიზარდა კიბერ შეტევები. ჰაკერებმა ძალიან კარგად იციან რომ COVID-19 გამოწვეული კრიზისის გამო ბევრი ადამიანი მუშაობს დისტანციურად. ამის გამო თანამშრომლების ნაწილი შედარებით მოდუნებულია, რაც ამცირებს მათ ყურადღებას და ზრდის მახეში გაბმის რისკს. მსგავსი შეტევებისგან თავდასაცავად ტექნოლოგიური საშუალებების გარდა მნიშვნელოვანია თანამშრომლების დატრენინგება, რათა მათ შეძლონ Phishing შეტევების იდენტიფიცირება და მოახდინონ შესაბამისი რეაგირება.

გასათვალისწინებელია რომ, ტრენინგებს ჰქონდეს განმეორებითი ხასიათი რათა თანამშრომლებს გამოუმუშავდეთ შესაბამისი რეფლექსები. BDO გთავაზობთ **Phishing-as-a-Service** (PhaaS) პროგრამას რომლის ფარგლებშიც ტრენინგებითა და თანამშრომლების მუდმივი სწავლებით ბიზნესებს შეუძლიათ დაამკვიდრონ კიბერ უსაფრთხოების კულტურა კომპანიაში .

ჩვენი მიდგომა

1 განვსაზღვრავთ Scope-ს

თქვენთან ერთად განვიხილავთ სხვადასხვა სცენარს და შევარჩევთ საუკეთესოს თქვენი ორგანიზაციისათვის.

2 Phishing შეტევის სიმულაცია

სიმულაციურ შეტევას არ ექნება არანაირი საოპერაციო შეფერხება

3 ანალიზი და რეპორტინგი

სიმულაციური შეტევის დროს ჩვენ არ ვაგროვებთ სენსიტიურ ინფორმაციას (მაგალითად პაროლებს). ჩვენი სიმულაციის მიზანია შეამოწმოს ადამიანის ქცევა და გაზარდოს მისი ცნობიერება.

4 უსაფრთხოების ტრენინგი

სიმულაციური შეტევის დასრულებისთანავე თანამშრომლები გაივლიან ტრენინგებს, რაც საშუალებას მისცემს მათ მარტივად დააიდენტიფიცირონ მსგავსი შეტევა და შეატყობინონ შესაბამის დეპარტამენტს

5 შეტევის ციკლის გამეორება

ცნობიერების ამაღლება განგრძობითი პროცესია. განმეორებითი Phishing სიმულაციებით ჩვენ მუდმივად გავზომავთ და გავზრდით ცნობიერების დონეს უსაფრთხოებაში. ამ გზით თანამშრომლებს მუდმივად ეცოდინებათ საფრთხეების შესახებ და იქნებიან ნაკლებად მოწყვლადი კიბერ შეტევების მიმართ.

უსაფრთხოების სერვისები და საჭიროებები

კიბერუსაფრთხოება კომპლექსურია და თავის თავში მოიცავს სხვადასხვა ფაქტორებს. შესაძლოა სწორედ ესაა იმის მიზეზი, თუ რატომ არ ან ვერ დგამენ ორგანიზაციები ქმედით ნაბიჯებს. სამწუხაროდ არ არსებობს აბსოლუტური უსაფრთოხება, ამიტომ არის მნიშვნელოვანი რისკებზე დაფუძნებული მიდგომა, რომელიც პირველ რიგში ფოკუსირებას მაღალი პრიორიტეტისა და რისკის კომპონენტზე აკეთებს.

BDO დაგეხმარებით შეარჩიოთ ყველაზე პრაგმატული და შესაფერისი კონტროლის მექანიზმი რომელიც უპასუხებს თქვენი ბიზნეს პროცესის გამოწვევებს.

კომპანიებს ვთავაზობთ ზუსტ რეკომენდაციებსა და ქმედით ნაბიჯებს, რომელიც უზრუნველყოფს მათი მონაცემებისა და სისტემების კონფიდენციალურობას, მთლიანობას, ხელმისაწვდომობასა და უსაფრთხოებას.

✔ სოციალური ინჟინერია ✔ ინფორმაციული უსაფრთხოების ტრენინგები	✔ Phishing სიმულაცია ✔ Live და Online ტრენინგები ✔ ტესტირება
✔ წვდომის მართვა ✔ სისუსტეების შემოწმება ✔ შეღწევადობის ტესტირება	✔ ლოგიკური წვდომის შემოწმება აპლიკაციებსა და ოპერაციულ სისტემებში ✔ Web გვერდებისა და IT ინფრასტრუქტურის ტექნიკური შემოწმება ✔ ეთიკური ჰაკინგი
✔ პოლიტიკები და პროცედურები ✔ კონტროლის მექანიზმების დანერგვა და რჩევები	✔ ორგანიზაციის საჭიროებებზე მორგებული პოლიტიკებისა და პროცედურების შექმნა/განახლება ✔ თქვენი კომპანიის მომზადება ISO 27001-ის სერტიფიცირებისათვის

ანზორ მეხრიშვილი
კიბერ და ინფორმაციული უსაფრთხოების მიმართულების ხელმძღვანელი

E-mail: amekhrishvili@bdo.ge
Tel.: +995 598 21 20 07

ნიკა ვაჭრიძე
ინფორმაციული უსაფრთხოების უფროსი ოფიცერი

E-mail: nvachridze@bdo.ge
Tel.: +995 598 98 41 43

BDO