

תיעוד

מגישים: שירלי בלאט, יעד בן-משה, הלל בוחבוט.

מבוא:

כיום כ-80% מבעיות הגנת המידע בחברות נובע מפעילות פנימית כלומר מפעילות העובדים. כאשר ברוב המקרים מדובר בשגיאה כתוצאה מחוסר ידע או תשומת לב של העובד. כתוצאה מכך, נוצר צורך עז בחינוך העובדים והסברה על מניעת בעיות אלו.

לינק לאתר: <http://www.haslishiya.com>

תיאור הכלי:

הכלי הינו אתר אשר מאפשר לחברות ואנשים פרטיים להתחבר ולשלוח דרכו מיילים/וואטספים המיועדים לחקוקת phishing.

מטרת הפרויקט היא הכשרה והעלאת מודעות בקרב עובדי חברות מפני הודעות phishing. היעד שלנו בפרויקט זה, הוא ביצוע שינוי בתפיסה החברתית תוך הכשרה וחינוך של עובדי החברות להגנה ברשת.

הכלי עונה על המטרה בכך שמאפשר לחברות לשלוח לעובדים שלהם מיילים/וואטספים המחקים phishing ובכך מעלה מודעות והסברה על כיצד להימנע ולהתנהל כאשר מקבלים מיילים והודעות כאלו. הכלי נועד לשקף לחברות את מצב התנהלות העובדים שלהם מול מיילים כאלו.

בנוסף, כחלק מחבילת ההגנה שהכלי שלנו מציע הוספנו תוסף אפליקציה שתסרוק עבור משתמש את תיבת הדואר הנכנס שלו ותמחק מיילים המכילים קבצים חשודים(כאשר מוגדר מראש מהו קובץ חשוד).

בעיות שנתקלנו בהם:

- בחירת סביבת העבודה והתשתית המתאימה לפרויקט.
- חשיבה כיצד ניתן לשמור נתונים ומשתנים היות והאתר נטען באופן סטטי.
- שימוש בג'ייסון לוקלי לא עבד בצורה טובה ולכן נאלצנו לעבור לmongo db וגם שם נתקלנו בבעיה היות והאתר לא באמת שלנו ועל כן לא הייתה שליטה על מתי ואם האתר נופל
- כיצד להעלות את האתר? האם לוקלי או לא. ניסינו דרך vercel והוא חסם לנו את שליחת המיילים ולכן הקמנו שרת.
- רצינו לתת אפשרות להעלאת קובץ עם מספר כתובות מיילים אך החלטנו שלא נעשה זאת היות ואין לנו דרך לבדוק את תוכן הקובץ ועל כן על מנת לשמור על עצמנו מווירוסים החלטנו שלא לאפשר זאת.
- רצינו לאפשר שליחת הודעות אסמס אך זה בתשלום ועל כן כרגע אנחנו לא תומכים בכך.
- על מנת לשלוח וואטספים נתקלנו בבעיה עם ההגדרות של וואטספ ועל כן אם חברה רוצה לתמוך בשליחת הודעות וואטספ עליה לבקש מכל אחד מהעובדים קודם לשלוח את ההודעה המצוינת באתר למספר המצוין שם ורק כך זה יעבוד.
- נתקלנו בבעיה של התאמת הרזולוציה של האתר לכלל המחשבים ולמכשירים סלולריים לבסוף הגדרנו התאמה של האתר לרזולוציות שונות.

חוזקות וחולשות הכלי:

חוזקות הכלי:

- יש אופציות גם למיילים וגם לוואטספים.
- הכלי שלנו מעלה בעיה קיימת ונותן גם מענה לפתרון.
- הכלי נותן סטטיסטיקות לחברה המאפשרות מעקב אחרי המצב של העובדים.
- שמירה על נתוני עבר.
- קיימת אפשרות ליצירת רשימת תפוצה אשר תקבל מייל/וואטספ.
- יש אפשרות לבחירת תבניות מעוצבות מראש.
- יש אפשרות להתנהל באתר מהפלאפון הנייד.

חולשות הכלי:

- אי אפשר לשלוח הודעות אסמס.
- על מנת לשלוח הודעות וואטספ על המשתמש לשלוח קודם הודעת וואטספ למספר כפי שהוצג באתר.
- זה אתר Fullstack ללא Backend אמיתי, אנחנו משתמשים ב API'S בעיקר.
- השרת עצמו יושב על המחשב שלנו.

תיאור עבודת הכלי:

הכלי מורכב מאתר ותוסף אפליקציה. האתר מאפשר הרשמה, חיבור, יצירת רשימות תפוצה שונות או הוספה של טלפונים/מיילים בודדים. דרך האתר ניתן לשלוח הודעות phishing מעוצבות בתבניות שונות המוכנות מראש או שהמשתמש יכול לעצב בעצמו או ללא תבנית כלל. כמו כן, ניתן לעקוב אחרי דיווחים וסטטיסטיקות שמציגות מי לחץ על קישור phishing ומי לא, דבר המאפשר הערכת מצב. האפליקציה היא תוסף מומלץ לאנשים המוצאים את עצמם נופלים קורבן ל phishing בכך שהיא מציעה סינון ראשוני של מיילים עם קבצים חשודים מתיבת הדואר הנכנס של המשתמש.

תיעוד הקוד והרכיבים המרכזיים בו:

*בקוד עצמו ישנן מספר הערות על דברים ספציפיים הנוגעים לקוד.

האתר נכתב בעזרת Next אשר מספק את ניתוב הדפים.

על מנת להקים מבנה נתונים ואתר השתמשנו בדוקרים להלן הסקריפטים:

- התחברות ל droplet

```
#!/usr/bin/env bash
wg pubkey < private
sudo ip link add wg0 type wireguard
sudo ip addr add 10.0.0.2/24 dev wg0
sudo wg set wg0 private-key ./private
sudo ip link set wg0 up
sudo wg set wg0 peer LUF0Fsndw7gWRQMmvmxrPIDLXqw+u7fYtIvfYr2DAFXI=
allowed-ips 10.0.0.1/32 endpoint 161.35.196.65:55767 persistent-
keepalive 20
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j
ACCEPT
sudo iptables -A INPUT -i wg0 -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -i wg0 -j DROP
```

- הסקריפט עבור הדוקר

```
FROM node:16-alpine
WORKDIR /app
ENV PATH /app/node_modules/.bin:$PATH
COPY package.json ./
COPY package-lock.json ./
RUN npm install --silent
RUN npm install -g dotenv env eslint eslint-config-next mongodb
@sendgrid/mail twilio @auth0/nextjs-auth0 react-chartjs-2 next
react react-dom
COPY . ./
CMD npm run build && npm start -- --port 80
```

האתר מורכב מכמה דפים עיקריים:

- [Index](#)
זהו הדף הראשי מבחינת Next , כלומר כאשר נפתח האתר זה הדף שיופיע.
- [Home](#)
זהו ה Dashboard בו יופיעו ההודעות שנשלחו והנתונים לגביו.
- [InsertEmails/Numbers](#)
אלו הדפים בהם ניתן להכניס מיילים ומספרים אליהם נרצה לשלוח הודעות. בנוסף, ניתן להגדיר בדפים אלו קבוצות תפוצה ולשמור אותן.

- [Email/textPhishing](#)
אלו הדפים שבהם אנו מבצעים את שליחת ההודעות עם התבניות המוצעות.
- [Email/textDetails](#)
דפים אלו מכילים את המיילים שנשלחו, מי לחץ ואת הסטטיסטיקות וגרף המייצג אותן.
- [Project](#)
דף בו יוצג קובץ תיעוד הפרויקט.
- [Help](#)
דף המכיל מדריך מפורט על השימוש באתר.
- [Clicked](#)
דף המגיע אליו לאחר לחיצה על הקישור המצורף להודעת phishing אשר מכיל קישורים לאתרי מידע בנוגע ל phishing.
- [Admin](#)
דף זה נועד למנהלי האתר, לשליטה על בסיס הנתונים.

האתר מורכב מכמה רכיבים מרכזיים:

components

- [Forms](#)
אלו הם הטפסים של המיילים וההודעות.
- [Templates](#)
אלו הם תבניות העיצוב של המיילים וההודעות.
- [Dashboard](#)
קוד זה מגדיר לנו את תצורת ה dashboard של המשתמש.
- [DataList](#)
זוהי מחלקה גנרית העוזרת לנו לייצר רשימות ממבנה נתונים נתון. אנו משתמשים בה בהכנסה של מיילים וטלפונים, בתצוגה של המיילים שנשלחו ועוד.
- [DataListResp](#)
זוהי מחלקה מקבילה ל DataList אשר מותאמת לשימוש במכשירים ניידים.

Api

- [Auth](#)
שימוש ב API חיצוני של auth0 על מנת לתחזק משתמשים לאתר.
- [EmailFormApi/ NumberFormApi](#)
הוספה והסרה של המיילים והמספרים לרשימות תפוצה.
- [EmailGroupApi/ NumberGroupApi](#)
יצירת קבוצות תפוצה.
- [GuideApi/insertGuideApi](#)
נועד לצורך תחזוקת מדריך המשתמש.
- [loggersApi](#)
מזהה כניסות דרך קישור phishing.
- [SendEmailApi](#)
משתמש ב API של SendGrid על מנת לשלוח מיילים עם אופציה לתבניות עיצוב מובנות.
- [sendTextApi](#)
משתמש ב API של Twilio על מנת לשלוח הודעות וואטספ עם אופציה לתבניות עיצוב מובנות.

ביבליוגרפיה:

אתרים חיצוניים שהשתמשנו בהם:

<https://www.digitalocean.com> שרת/Droplet עליו יושב האתר

<https://www.mongodb.com/home> מבנה נתונים – Docker של MongoDB

ספריות ורכיבי קוד:

<https://nextjs.org> - Next JS

<https://nodejs.org/en> - Node JS

<https://reactjs.org> - React

<https://reactjs.org/docs/react-dom.html> - React-Dom

<https://auth0.com> - Auth0

<https://sendgrid.com> - Sendgrid

<https://react-chartjs-2.js.org> - React charts

<https://www.chartjs.org> - Chart JS

<https://www.npmjs.com/package/dotenv> - Dotenv

<https://www.mongodb.com/home> - Mongodb

<https://www.twilio.com> - Twilio

[/https://www.gnu.org/software/bash](https://www.gnu.org/software/bash) - Bash

עיצוב:

https://dribbble.com/tags/phishing_illustration - תמונת דף הבית

<https://www.throttlenet.com/blog/security/make-your-it-> - תמונת הBusted
[/network-a-no-phishing-zone](https://www.throttlenet.com/blog/security/make-your-it-network-a-no-phishing-zone)

<https://www.shutterstock.com/search/phishing-> - תמונת הלוגו של הפרויקט

[logo](#)

<https://in.bgu.ac.il/en/pages/default.aspx> - תמונת לוגו אוניברסיטת בן גוריון