STADT ESSEN

Erfahrungen im Rahmen der Sensibilisierung bei einer Phishing-Simulation

10. Kommunaler IT-Sicherheitskongress, Berlin, 22. April 2024

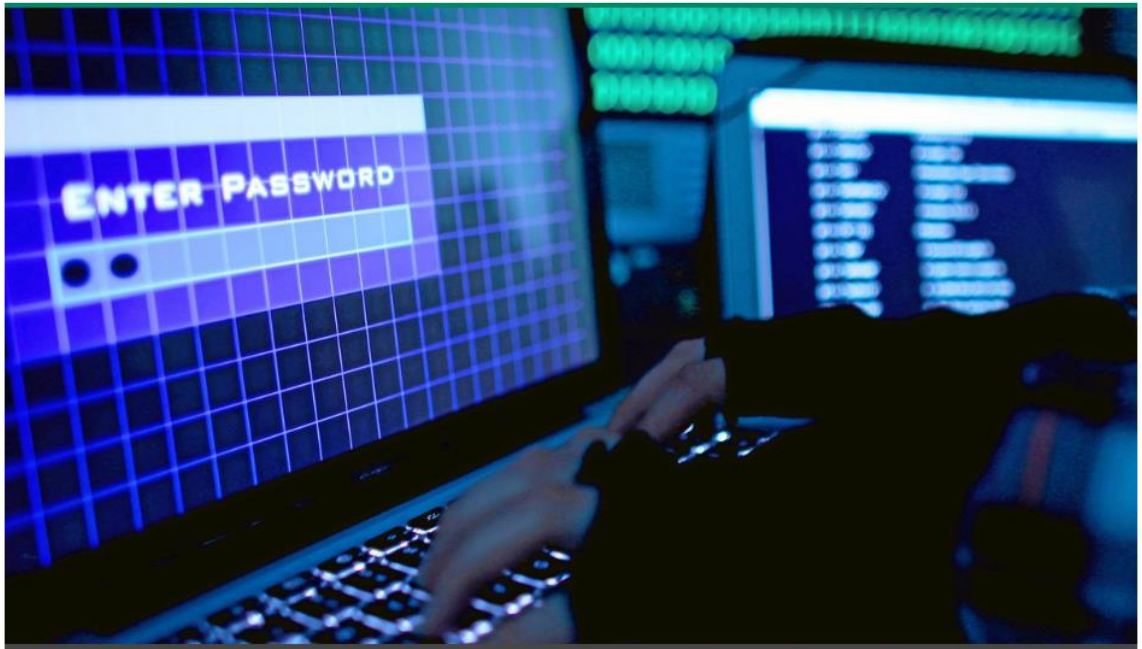

STADT ESSEN
Digital
Your files are encrypted!
Ihre Dateien sind verschlüsselt!
Pay 1,000 Bitcoins
to decrypt the data.
Bezahlen Sie 1.000 Bitcoins
um die Daten zu entschlüsseln.
Time left
Verbleibende Zeit
9:12:23
STADT ESSEN
Digital

CYBER-KRIMINALITÄT

Stadt Essen wehrt Hackerangriff ab - die Polizei ermittelt NRZ+

Aktualisiert: 04.10.2023, 09:31 | Lesedauer: 3 Minuten

Jörg Maibaum und Wolfgang Kintscher



An Passwörter kommen und sich in die IT-Systeme einzuschleichen – das war offenbar das Ziel der Angreifer. Die Stadt Essen reagierte prompt.

Foto: Oliver Berg / picture alliance / dpa

ESSEN. Ein Hackerangriff auf die Stadt Essen ist offenbar frühzeitig bemerkt worden. Schlimmeres konnte verhindert werden, die IT war auf Zack.

NRZ
04.10.2023

Wir wissen, was passieren kann. Wenn wir uns nicht vorbereiten, handeln wir **fahrlässig**.

Investitionen in Informationssicherheit sind **günstiger** als ein wochenlanger Notbetrieb.

„Ein erfolgreicher Cyberangriff findet statt. Fraglich ist **wann**.“ Quelle: BSI

STADT ESSEN

Erfahrungen im Rahmen der Sensibilisierung bei einer Phishing-Simulation

Kurzüberblick über die Bedrohungslage

Phishing

Angreifer

Phishing zielt darauf ab, sensible und personenbezogene Daten zu erhalten

Trojaner & Würmer
Informationspreisgabe

Verschicken falscher Nachrichten mit Anhängen oder Links zu Online-Shops, Sozialen Netzwerken, Bezahldiensten etc.

Opfer

Opfer geben nichtsahnend persönliche und vertrauliche Informationen ein, klicken auf Anlagen

Die Lage der IT-Sicherheit in Deutschland 2023
im Überblick*

Ransomware

ist weiterhin die größte Bedrohung.

Top-3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Phishing	***Ransomware*** Abhängigkeit innerhalb der IT-Supply-Chain Schwachstellen, offene oder falsch konfigurierte Onlineserver	***Ransomware*** APT Schwachstellen, offene oder falsch konfigurierte Onlineserver

*Die Lage der IT-Sicherheit in Deutschland (https://www.bsi.bund.de/)

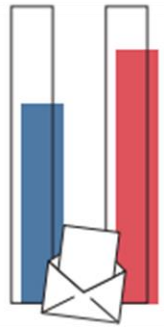
Die Lage der IT-Sicherheit in Deutschland 2023
im Überblick*

Ransomware

ist weiterhin die größte Bedrohung.

66%

aller **Spam-Mails** im Berichts-zeitraum waren Cyberangriffe:
34 % Erpressungsmails,
32 % Betrugsmails



84%

aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

*Die Lage der IT-Sicherheit in Deutschland (https://www.bsi.bund.de/)

Erfahrungen im Rahmen der Sensibilisierung bei einer Phishing-Simulation

Sensibilisierung

Sensibilisierungsmaßnahmen

Sensibilisierung

Phishing-Simulation 1

Eckdaten zur Phishing-Simulation

Auftrag	**Mehrere Simulationen inklusive Auswertungen**
Zeitraum einer Simulation	**vier Wochen**
Ø Versandte E-Mails	**40.000**
Ø Teilnehmendenzahl	**11.500**
Ø Mails pro TN	**3,5**

Phishing-Simulation

Zielsetzungen

Ziel der „Trigger“-E-Mails

- Anhänge zu öffnen
- Sensible Daten preisgeben
- Unsichere Webseiten besuchen

Ziel der Simulation

- Beschäftigte werden bei falschem Verhalten auf Informationsseite geleitet und über das richtige Verhalten aufgeklärt
- Eigene Erfahrung machen

„Ich habe das angeklickt,
aber es ist ja nichts passiert“

STADT
ESSEN

„Das Dokument war leer, also habe ich mir gedacht: Zum Glück. War wohl SPAM“

STADT ESSEN

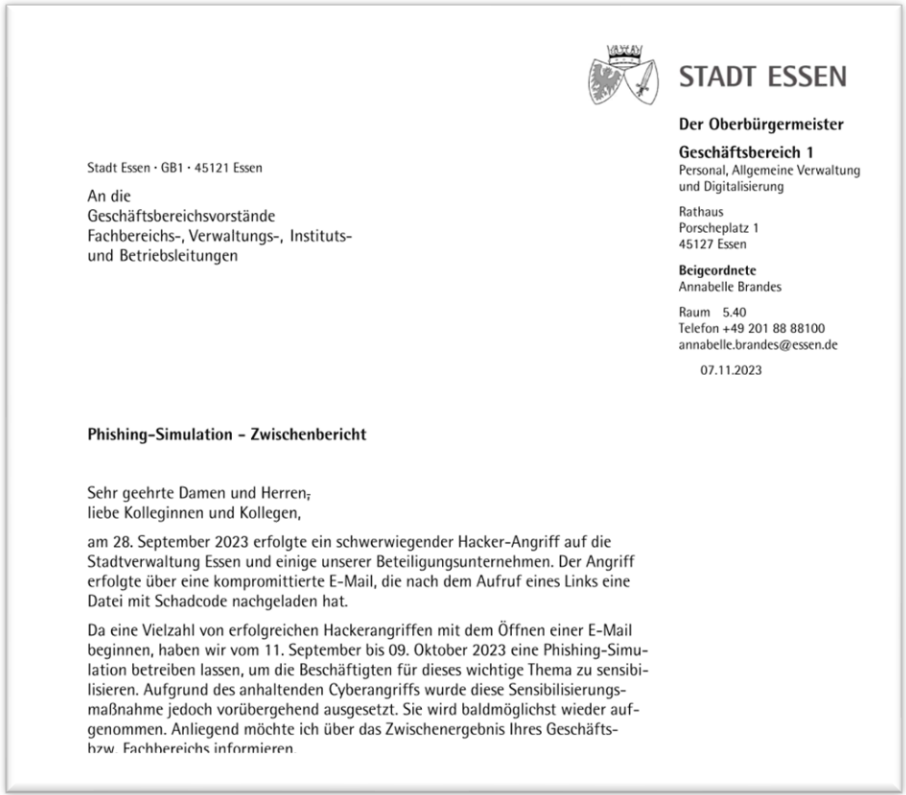
!!!

Information und Kommunikation

Ergebnisse werden detaillierter geteilt mit …

- Verwaltungsvorstand
- Chief Information Security Officer (CISO)
- Fachbereichsleitungen
- Beschäftigten
- Unternehmen im Konzern Stadt Essen

Information für Führungsebene…



STADT ESSEN

Der Oberbürgermeister

Geschäftsbereich 1
Personal, Allgemeine Verwaltung und Digitalisierung

Rathaus
Porscheplatz 1
45127 Essen

Beigeordnete
Annabelle Brandes

Raum 5.40
Telefon +49 201 88 88100
annabelle.brandes@essen.de

07.11.2023

Stadt Essen · GB1 · 45121 Essen

An die
Geschäftsbereichsvorstände
Fachbereichs-, Verwaltungs-, Instituts-
und Betriebsleitungen

Phishing-Simulation – Zwischenbericht

Sehr geehrte Damen und Herren,
liebe Kolleginnen und Kollegen,

am 28. September 2023 erfolgte ein schwerwiegender Hacker-Angriff auf die Stadtverwaltung Essen und einige unserer Beteiligungsunternehmen. Der Angriff erfolgte über eine kompromittierte E-Mail, die nach dem Aufruf eines Links eine Datei mit Schadcode nachgeladen hat.

Da eine Vielzahl von erfolgreichen Hackerangriffen mit dem Öffnen einer E-Mail beginnen, haben wir vom 11. September bis 09. Oktober 2023 eine Phishing-Simulation betreiben lassen, um die Beschäftigten für dieses wichtige Thema zu sensibilisieren. Aufgrund des anhaltenden Cyberangriffs wurde diese Sensibilisierungsmaßnahme jedoch vorübergehend ausgesetzt. Sie wird baldmöglichst wieder aufgenommen. Anliegend möchte ich über das Zwischenergebnis Ihres Geschäfts- bzw. Fachbereichs informieren.

RISIKOBEWERTUNG PHISHING-AWARENESS

G DATA academy

Phishing ist eine Angriffsmethode, in der Cyberkriminelle über Täuschung Ihrer Mitarbeiter technische Sicherheitsmaßnahmen umgehen, um an Zahlungs- und Zugangsdaten zu gelangen. Wir haben die Sensibilisierung Ihrer Mitarbeiter gegenüber Phishing-Attacken gemessen und bewertet. In diesem Bericht erhalten Sie die Ergebnisse.

Durchführung

Versendete E-Mails	Durchführungszeitraum	Teilnehmeranzahl
[redacted]	11.09.2023 - 09.10.2023	[redacted]

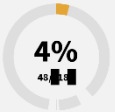
Ergebnis

[redacted]

HOHES RISIKO

Ein signifikanter Teil Ihrer Mitarbeiter erkennt schädliche E-Mails nicht. Dadurch erhöhen sie enorm das Risiko einer erfolgreichen Attacke durch Phishing, inklusive seiner wirtschaftlichen Konsequenzen für Ihr Unternehmen.

Sensible Daten preisgegeben



Wenn Ihr Mitarbeiter Zahlungs- und Zugangsdaten durch eine gefälschte Anfrage preisgibt, nutzt der Angreifer die Daten für sich aus. Dies führt zu einem finanziellen und wirtschaftlichen Schaden ihres Unternehmens.

Anhänge geöffnet

[redacted]

Wenn Ihr Mitarbeiter einen infizierten Anhang öffnet, laden Angreifer Schadsoftware auf das Endgerät. Sie infiltrieren das Netzwerk, verschlüsseln zentrale Bereiche und legen dadurch elementare Prozesse im Unternehmen lahm.

Top 3 der gefährlichsten Angriffe

Mit den drei folgenden Stories konnten wir Ihr Unternehmen erfolgreich angreifen:

[redacted]	**Firmeninterne Gehaltsübersicht mit Anhang** Die Zielperson wird durch veröffentlichte Gehaltsübersichten und geheime Protokolle dazu bewegt ein Word-Dokument zu öffnen.
4%	**Neues 2FA-Verfahren** Die Zielperson wird unter dem Vorwand von Sicherheitsverbesserungen (Einführung 2-Faktor-Authentifizierung) auf eine Webseite gelockt, um dort persönliche Daten einzugeben.
0%	**Neue DMS-Dokumente** Die Zielperson wird unter dem Vorwand von neu verfügbaren Dokumenten auf eine fingierte Seite des DMS-Web-Clients "DOXiS4 webCube" gelockt, um dort ihre Anmeldedaten einzugeben.

Handlungsempfehlungen

Der reflektierte Umgang Ihrer Mitarbeiter mit alltäglicher E-Mail-Kommunikation hat einen entscheidenden Einfluss auf die IT-Sicherheit Ihres Unternehmens.

E-Mails geöffnet

Ihre Mitarbeiter können bereits erste Anzeichen einer Phishing-Mail erkennen, ohne sie öffnen zu müssen – wenn sie geschult sind. Bilden Sie Ihre Mitarbeiter weiter und zeigen Sie Ihnen die ersten Indikatoren betroffener E-Mails. So tragen Sie dazu bei, vermehrte Attacken oder die Weitergabe der E-Mail-Adresse an weitere Angreifer zu verhindern.

Unsichere Webseite besucht

Ihre Mitarbeiter können den Klick auf einen infizierten Link vermeiden – wenn sie die E-Mail im Vorhinein als gefährlich eingestuft haben. In entsprechenden Schulungen und Weiterbildungen lernen sie, die Indikatoren zu erkennen und entsprechenden Links mit Skepsis zu begegnen.

Sensible Daten preisgegeben

Bringen Sie Ihren Mitarbeitern bei, den Inhalt ihrer Mails zu reflektieren und zu hinterfragen. Ihre Mitarbeiter sollten beim Bearbeiten ihrer E-Mails sensibilisiert sein und sich stets fragen: Ergibt es Sinn, dass mich dieser Kollege nach Kreditkarteninformationen fragt? Ist die Seite, auf der ich meine Zugangsdaten eingeben soll, vertrauenswürdig?

Anhänge geöffnet

Dass Ihre Mitarbeiter sich bei Kollegen informieren, ob sie eine verdächtige Datei tatsächlich verschickt haben, muss zur Selbstverständlichkeit werden. Das setzt voraus, dass IT-Sicherheit ein wesentlicher Bestandteil Ihrer Unternehmenskultur ist. Machen Sie IT-Sicherheit zu einem Thema, das nicht nur die entsprechende Abteilung betrifft, sondern alle Mitarbeiter.

Information für Beschäftigte …

- Sofortinformation im Rahmen der Phishing-Simulation
  - Wenn sensible Daten preisgegeben wurden, direkter Hinweis durch eine Informationsseite
- Meldungen wurden wie „echte“ Fälle behandelt
- Die Fachbereiche haben ihre Beschäftigten intensiver informiert und Regelungen kommuniziert
- Überarbeitung DA Informationssicherheit

Mit Blick auf die Beschäftigten …

- Einfacher Zugang zu Informationen und Schulungsinhalten
- Fachschulungen für Fachpersonal
- Informationssicherheit als Baustein im Geschäftsprozess
- Sensibilisierungsmaßnahmen beginnen in jedem Team
- Verhalten und Auswirkungen besprechen
- Erfahrungen helfen, Flyer nicht
- Einfache Nutzungsmöglichkeiten führen zur Nutzung!

Persönliche Ansprache wurde fokussiert!

Sensibilisierung

Phishing-Simulation 2

Investieren lohnt sich,
Hoffen nicht!

STADT
ESSEN

Vielen Dank!


STADT
ESSEN
Digital
Patrick Rauch
Informationssicherheits-
beauftragter (ISB)
Digitale Verwaltung
Lindenallee 6
45127 Essen
Tel.: +49 201 88-88123
E-Mail: patrick.rauch@
digital.essen.de
www.essen.de
STADT
ESSEN