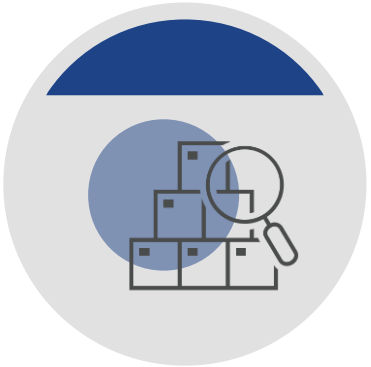
Halbjahresbericht

zur Informationssicherheit in der LH Wiesbaden

Die vier Säulen der Informationssicherheit



PRÜFUNG

Initiierung und Prüfung der Realisierung von Sicherheitsmaßnahmen

STEUERUNG

Steuerung des Informations-sicherheits-prozesses

SCHULUNG

Initiierung und Koordination von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit

UNTERSUCHUNG

Untersuchung von Sicherheitsvorfällen

Initiierung und Prüfung der Realisierung von Sicherheitsmaßnahmen

- Intensivierung der Zusammenarbeit mit der Wivertis
- Einrichtung von DMZ (DeMilitarized Zones) im Netz der LHW
- Netztechnische Trennung von internen und externen Services
- Projektstart zum KDLZ-CS[1] mit der ekom21
  (Kommunales DienstLeistungsZentrum-CyberSicherheit)

[1] https://www.ekom21.de/loesungen/kdlz-cs/

Steuerung des Informationssicherheitsprozesses

- Etablierung eines CERT (Computer Emergency Response Team)
- Etablierung eines zentralen Freigabeprozesses des IT-Managements unter Berücksichtigung der Empfehlungen des ISB, DSB und LM
- Neue Passwortrichtlinie auf Basis aktueller Forschungsergebnisse
- Bessere Koordination der Beteiligung von ISB & DSB bei Beteiligungs- und Vergabeverfahren innerhalb der LHW

Initiierung und Koordination von Sensibilisierungs- und Schulungsmaßnahmen

- Bereitstellung einer Wissensplattform[2] zur eigenverantwortlichen Weiterbildung der Mitarbeitenden zu Informationssicherheitsthemen
- Zeitnahe Information aller Mitarbeitenden bei drohenden Gefahren
- Zusätzliches, optionales Informationsangebot zu informationssicherheitsrelevanten Themen im privaten Umfeld (Banking-Trojaner, etc.)

[2] https://www.bits.intern.wiesbaden.net/

Untersuchung von Sicherheitsvorfällen

- schwerwiegende Sicherheitslücken, die uns getroffen haben

log4j – Schwachstelle(n)[3]

- bekannt geworden im Dezember 2021
- Lücke führte zu einer direkten Übernahme des betroffenen Rechners
- erst nach mehreren Versuchen gab es eine abgesicherte Version

- bei uns waren über 50 Anwendungen/Services betroffen
- Abschaltung aller extern erreichbaren Anwendungen
- manche Services erst Ende März 2022 wieder abgesichert online

[3] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Schwachstelle-log4Shell-Java-Bibliothek/log4j_node.html

Follina – Microsoft Office Vorschau[4]

- bekannt seit Anfang Mai 2022
- Office-Dokumente mit Schadcode wurden unabhängig von den Sicherheitseinstellungen bei der Erstellung der Vorschauansicht im Windows-Explorer ausgeführt

- betraf die gesamte LHW
- Workaround durch setzen von Windows-Registry-Einträgen umgehend umgesetzt
- Patch war erst mit dem Juni-Patchday von Microsoft verfügbar

[4] https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2022/2022-224508-1032.pdf

Untersuchung von Sicherheitsvorfällen

- schwerwiegende Sicherheitslücken, die uns getroffen haben
- Phishing-Versuche

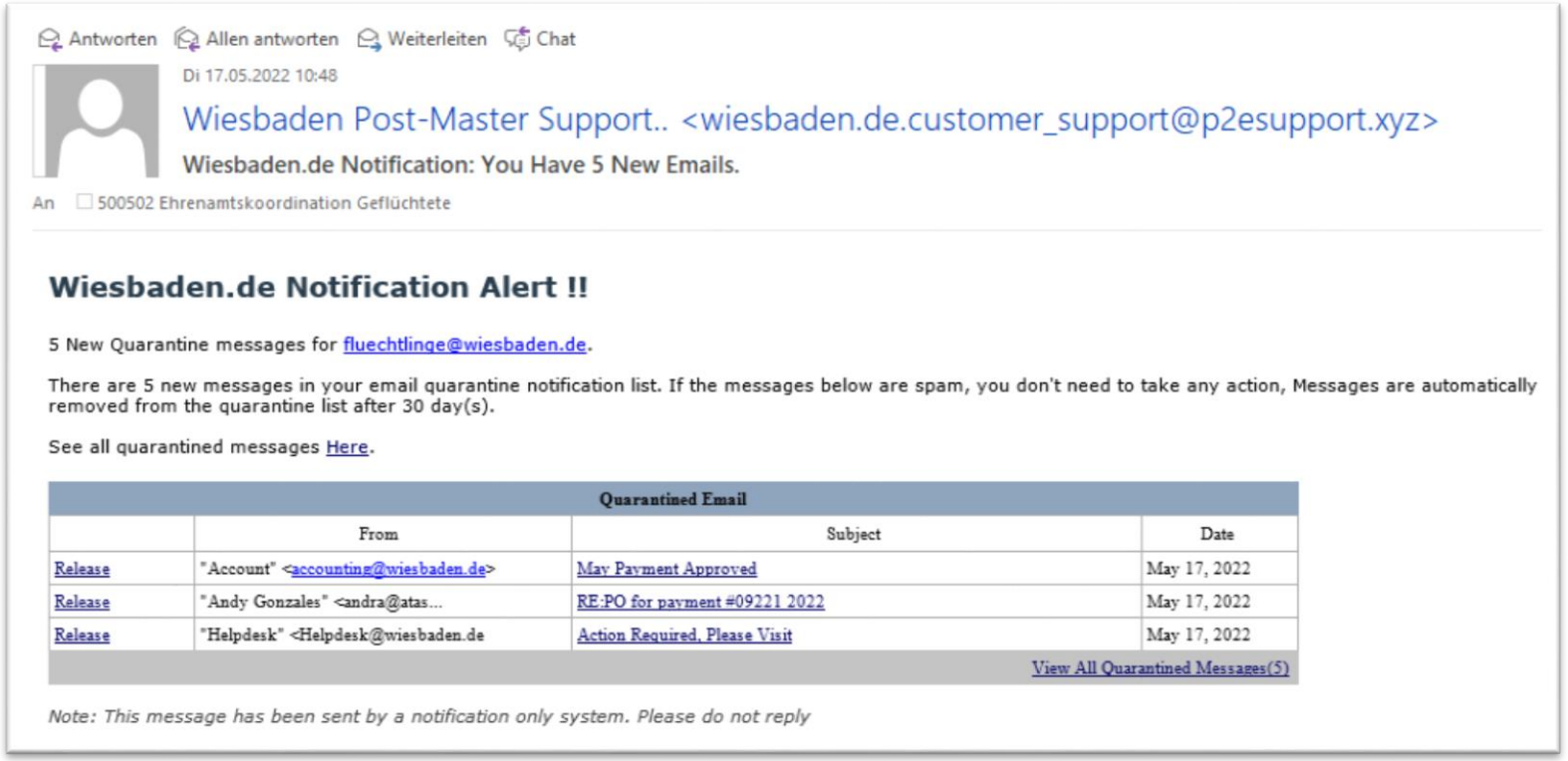
Outlook-Harvesting I

- Übernahme des privaten Mailpostfachs (T-Online) eines ehrenamtlichen Magistratsmitglieds im November 2021
- Entwendung von E-Mails, u.a. über ein Projekt von LHW und Wi-Bau aus dem August 2021

- Nutzung des Mailverlaufs, um im Namen des LHW-Mitarbeitenden Links zum Download von Schadsoftware an die Wi-Bau Wiesbaden zu verschicken

Versuche von Postfachübernahmen

- Phishingmail an das (alte) Organisationspostfach zur Flüchtlingskoordination



Antworten Allen antworten Weiterleiten Chat

Di 17.05.2022 10:48

Wiesbaden Post-Master Support.. <wiesbaden.de.customer_support@p2esupport.xyz>

Wiesbaden.de Notification: You Have 5 New Emails.

An 500502 Ehrenamtskoordination Geflüchtete

Wiesbaden.de Notification Alert !!

5 New Quarantine messages for fluechtlinge@wiesbaden.de.

There are 5 new messages in your email quarantine notification list. If the messages below are spam, you don't need to take any action, Messages are automatically removed from the quarantine list after 30 day(s).

See all quarantined messages Here.

Quarantined Email			
	From	Subject	Date
Release	"Account" <accounting@wiesbaden.de>	May Payment Approved	May 17, 2022
Release	"Andy Gonzales" <andra@atas...	RE:PO for payment #09221 2022	May 17, 2022
Release	"Helpdesk" <Helpdesk@wiesbaden.de	Action Required, Please Visit	May 17, 2022
			View All Quarantined Messages(5)

Note: This message has been sent by a notification only system. Please do not reply

Outlook-Harvesting II

- Abfluss von Mailverläufen zwischen der LHW, der Polizei Hessen und einem Ingenieurbüro

- Nutzung eines Mailverlaufs vom Februar 2022, um im Namen des LHW-Mitarbeitenden Links zum Download von Schadsoftware an den Mitarbeitenden im Polizeipräsidium Westhessen in Wiesbaden zu verschicken

Untersuchung von Sicherheitsvorfällen

- schwerwiegende Sicherheitslücken, die uns getroffen haben
- Phishing-Versuche
- Schwachstellenscans

Schwachstellenscans externer Webapplikationen

- seit Ende April 2022 in unseren Log-Dateien sichtbar
- Einsatz des Tools FFUF (Fuzz-Faster-yoU-Fool)[5]
- Quell-IP-Adressen aus dem Bereich der Russischen Föderation

- Betrifft „nur“ Webdienste, welche von außen erreichbar sind (WIZEMA-Portal, wahlergebnisse.wiesbaden.de, etc.)

[5] https://github.com/ffuf/ffuf/

Fragen?

Dr. rer. nat. Julian Heinrich

Informationssicherheitsbeauftragter

Landeshauptstadt Wiesbaden

Telefon: 0611 31-7810

E-Mail: dr.julian.heinrich@wiesbaden.de

INNOVATION FINDET Stadt

Amt für Innovation, Organisation und Digitalisierung