Department Report

MEETING DATE: September 16, 2024

FROM: Georges Bayard, Director, Information Technology

SUBJECT: Department of Information Technology – August 2024 Activity Report

DEPARTMENT HIGHLIGHTS

The following report provides the highlights of activity within the Information Technology Department for the reporting period from August 1 - August 31, 2024.

1.   The paperless Personnel Action Request (PAR) form in New World ERP is now in testing for all departments.

2.   Developing a paperless requisition and purchase order process between New World ERP and Laserfiche.

3.   Developing new, consolidated IT Service Desk ticket templates, to reduce the number of available items for users to choose from. This will help provide more complete information for IT staff to work on any given issue, while simplifying the request process for the users.

4.   The weekly scans of the City's network by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) Cyber Hygiene program have found no vulnerabilities that could be exploited by malicious actors via the Internet. See report below.

5.   As an added security feature, we implemented Proofpoint's URL Isolation for any links in email messages for key City personnel with access to sensitive information, i.e. department heads, managers, Mayor and City Council, IT, HR, Finance. This results in any links clicked in email messages opening in an isolated browser window, to prevent any potential malicious activity. Clicking on an "Exit" button after verifying that the site is legitimate provides full functionality.

6.   Monthly KnowBe4 simulated phishing test results:

      a.   **August:** Links clicked: 5; attachments opened: 1; QR codes scanned: 0. Phish-prone users (vulnerable to phishing attacks): 3.31% (slightly down from 3.35% during the previous month's campaign).

Despite the slight increase in risky behavior in response to simulated phishing tests this past month, the overall online behavior of City personnel remains more cautious than the average KnowBe4 customer. Users who take actions they shouldn't continue to be assigned remedial training to reinforce secure handling of emails. Use of Artificial Intelligence (AI) in current real phishing campaigns significantly increases the effectiveness of attackers' messaging. We will continue to adjust our phishing campaigns and training content accordingly to encourage constant good cyber hygiene.

August 2024

DEPARTMENT	CURRENT PERIOD	FY 2024 YTD	FY 2024 BUDGET
Administration	15	131	-
Community & Recreation Services	5	84	-
Development & Neighborhood Svcs.	9	163	-
Finance	13	97	-
Fire Rescue	9	73	-
Information Technology	2	27	-
Public Works	3	39	-
Purchasing	2	25	-
Youth Programs	8	40	-
Total Service Desk Requests	**66**	**679**	**600**

CYBER HYGIENE

REPORT CARD

City of Greenacres

0
0
Hosts with unsupported software

0
Potentially Risky Open Services

0%
No Change in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

July 31, 2024 — August 28, 2024
Completed host scan on all assets

No vulnerability scans yet
Last vulnerability scan on all hosts

ASSETS OWNED

32 ⊙
No Change

ASSETS SCANNED

32 ⊙
No Change
100% of assets scanned

HOSTS

0 ⊙
No Change

SERVICES

0 ⊙
No Change

VULNERABLE HOSTS
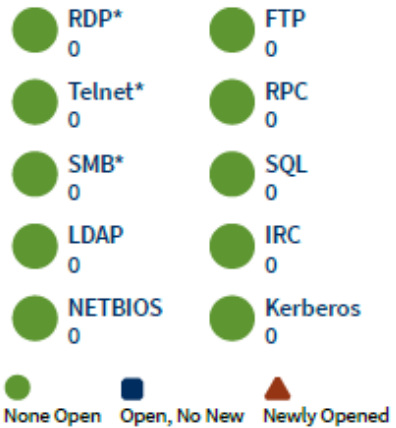
0 ⊙
No Change
0% of hosts vulnerable

VULNERABILITIES

0 ⊙
No Change

VULNERABILITIES

SEVERITY BY PROMINENCE

0
CRITICAL
0 RESOLVED
0 NEW

0
HIGH
0 RESOLVED
0 NEW

0
MEDIUM
0 RESOLVED
0 NEW

0
LOW
0 RESOLVED
0 NEW

VULNERABILITY RESPONSE TIME

0
DAYS

0 Days   15+ Days

MAX AGE OF ACTIVE CRITICALS

0
DAYS

0 Days   30+ Days

MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP*
0

FTP
0

Telnet*
0

RPC
0

SMB*
0

SQL
0

LDAP
0

IRC
0

NETBIOS
0

Kerberos
0

None Open   Open, No New   Newly Opened
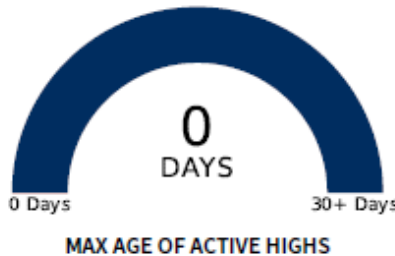
Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

* Denotes the possibility of a network management interface.