Implementation of Faculty-facing Cybersecurity Measures to Prevent Successful Ransomware Attacks

Jim Yukech – AVP/CIO, YSU

Justin Bettura– Associate Director, Deputy CISO

April 6, 2022

YOUNGSTOWN STATE UNIVERSITY

Background

- Several successful “high profile” ransomware attacks in 2021 focused our Cybersecurity efforts on the Ransomware threat.
  - YSU ITS Security Team developed a Ransomware Remediation plan to harden our digital environment to meet Cybersecurity best practices over an 18 month period (May 2021 through November 2022).
  - The FBI, a Regional Cybersecurity consultant (Trusted Sec) and the Kent State University IT Security Team were all consulted in the development of our Ransomware Remediation plan.
  - Mike Christman, Asst. Director of Criminal Justice Information Services Division, co-presented regarding the impending Ransomware threat at the September 2021 Board of Trustees meeting. Jim Yukech presented our Remediation Plan which was endorsed by the Board of Trustees.
  - Each of the other IUC universities have developed similar plans.

Malware Threats

- Short for “malicious software,” refers to any intrusive software developed by cybercriminals (often called “hackers”) to steal data and damage or destroy computers and computer systems.
- Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and **ransomware**.
- Recent malware attacks have exfiltrated data in mass amounts.
- ***Phishing via email is the most common hacker approach for breaching user access credentials.***

Ransomware Threat in Higher Education

- Higher Education is a significant target for intellectual property due to its' traditionally collegial open exchange of information – both internally among colleagues and externally with peer universities and the private sector.
- As such, attacks against universities were up 100 percent in 2020 over 2019, and doubled again from 2020 to 2021, with an average ransom demand of nearly $600,000 with total remediation costs exceeding $1M per event.

IUC CIO Survey Results

Surveyed the State universities in Ohio regarding faculty-facing Ransomware remediation efforts. Eleven of the 14 responded.

- **Admin Privileges: 55%** (6/11) eliminated or limiting admin privileges
- **MFA: 100%** have either implemented or are in-process of implementing
- **University e-mail: 91%** (10/11) enforce use of university e-mail
- **University storage: 36%** (4/11) enforce use of university storage

https://reporting.alchemer.com/r/387974_6234a70646a149.94708973

We need your help…

Four significant faculty-facing remediation efforts are in-process to further mitigate the ransomware threat: (timeframe in parenthesis):

- **Reducing the potential threat caused by breached administrative privileges** through advanced cyber tools and limiting these advanced privileges to just one primary device for full-time faculty members ***(immediate, implemented by end of April 2022)***
- **Significantly reducing the threat caused by breached standard access credentials** by implementing multifactor authentication (MFA) campus-wide ***(in-process, staff and students completed, faculty fully-implemented by end of May 2022)***
- **Enforcing the University's "Acceptable Use" policy** by migrating all faculty, staff, contractors and Board of Trustee members to University protected email (i.e. ysu.edu) for conducting university business ***(targeted for Fall 2022-Spring 2023)***
- **Enforcing the University's "Network Storage" policy** by ensuring that all faculty, staff, contractors and Board of Trustees members are using encrypted cloud storage (i.e. MS-OneDrive) for storage of university and faculty data ***(targeted for Fall 2022-Spring 2023)***

Questions ?

YOUNGSTOWN
STATE
UNIVERSITY