CITY OF POCATELLO
CITY COUNCIL LIAISON/WORK SESSION CLARIFICATION

February 20, 2020 · 2:00 PM
Paradice Conference Room | 911 North 7th Avenue

City Hall is accessible to persons with disabilities. Program access accommodations may be provided with three (3) days' advance notice by contacting Skyler Beebe at sbeebe@pocatello.us; 208.234.6248 or 5815 South 5th Avenue, Pocatello, Idaho.

1. **ROLL CALL**
2. **WORK SESSION CLARIFICATION/DISCUSSION**

   Discussion to clarify agenda items presented at the February 13, 2020 Work Session.
3. **ENERGY TASK FORCE CLARIFICATION**

   Discussion regarding the Energy Task Force will be held.
4. **EMAIL CYBERSECURITY PROTOCOL**

   Discussion regarding the City's email cybersecurity protocol will be held.

   Documents:

   CYBERSECURITY-PROTOCOL.PDF
5. **CITY ACTIVITIES UPDATE—COUNCIL**
6. **CITY ACTIVITIES UPDATE—MAYOR**
7. **CITY COUNCIL REPORTS REGARDING CITY BOARDS/COMMISSIONS**
8. **ADJOURN**

EMAIL PROCESSING
(Incoming – Outgoing)

- Individual outside the City sends someone inside the City an email
    - The email enters the network through a device called a boundary switch that looks at the type of data coming in and directs it to the appropriate computer
    - If the data is an email, the data is then sent through a computer called a firewall that does some initial security checks of the data to ensure it passes certain security criteria.
        - This first firewall segregates the email to a location separated from the rest of the network to protect the integrity of the City's network from a potential dangerous email that may release dangerous content that is not recognized by any of the security elements in place…often referred to as a "zero-day" event
    - If it passes these checks it is sent to an email dedicated computer called a secure mail transfer protocol (SMTP) gateway

- Email arrives at the City's SMTP email gateway
    - The gateway looks at the email and determines if recipient is a valid email address in our system
    - If the email is determined to be a valid email, it is further evaluated by MailMarshal software on the gateway
    - If the addressee is not valid, the gateway rejects the email

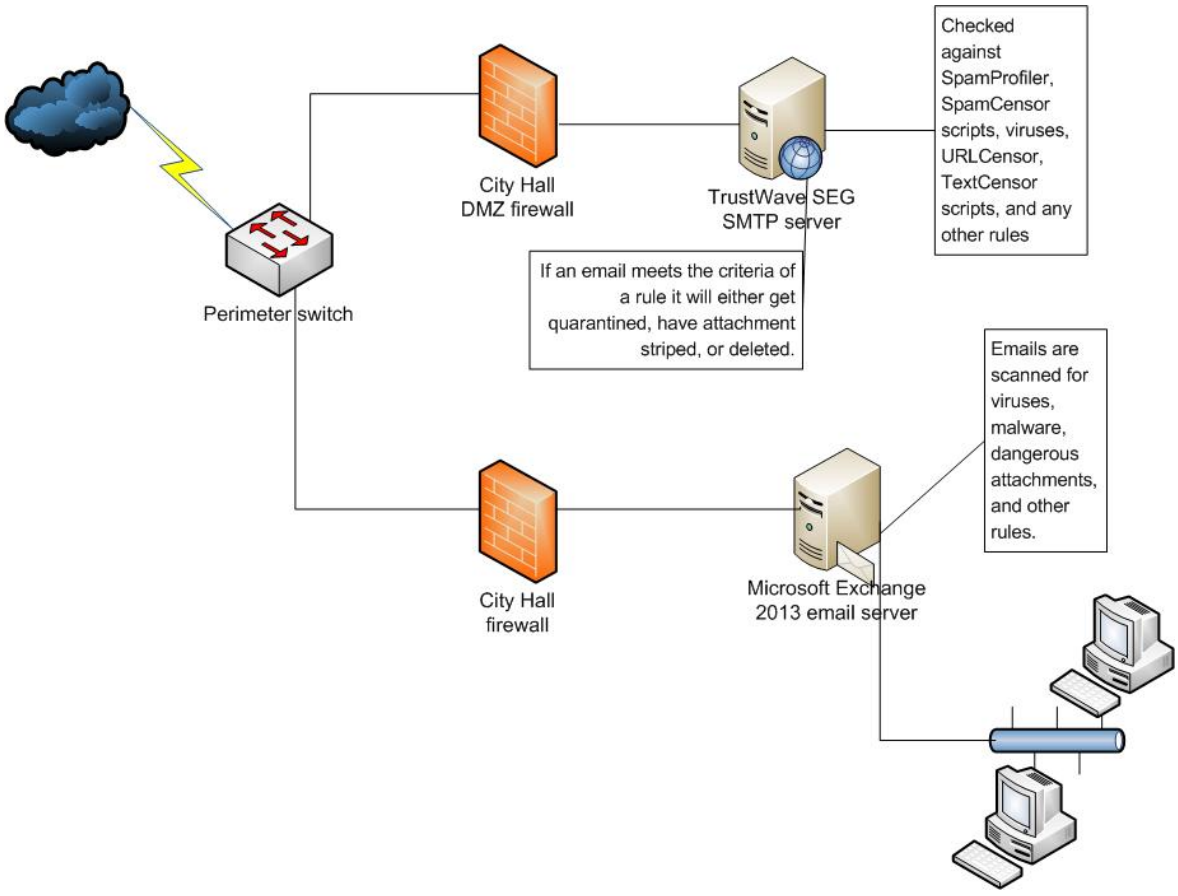
- Email evaluation by the MailMarshal
    - All inbound and outbound email goes through the MailMarshal. At this stage, the MailMarshal applies Spam checks, virus scans, and any of several other rules to messages.
    - Next, the MailMarshal opens each email, expanding any attached archive or compressed files. The system then checks each part of the email against rules that are enabled, including Spam scripts, known dangerous links, restricted text scripts, and any other rules that are enabled. Rules can be altered in MailMarshal based on policy and risk assessments. The MailMarshal comes preconfigured with default industry-standard options, and changes to those options are based on specific threats.
    - After the MailMarshal evaluates each email component against the rules, it determines whether to accept, modify, or quarantine the email. (It may also outright delete an email if it contains a known threat signature.)

        - **Accepted email** is passed to the appropriate recipients via a specialized computer called the Exchange Server that handles the delivery of email in the network (the Exchange Server may redirect an email at this point if the recipient has a redirect set up for the email address).

        - **Modified email** may be delivered to recipients with dangerous attachments removed.

        - **Quarantined email** is email that may be virus-laden, and/or email that violates other policies and is held until released or after set expiration times. The MailMarshal will notify system administrators of specific actions and notify end-users of quarantined email. Users may contact the Help Desk and request a manual review and release if the email is deemed safe for release.

- Email administrators can review email processing history for a message and view and release any quarantined message. This process is followed in a similar manner for outbound email. Internal email does not go through the MailMarshal process and is totally handled by the Exchange Server.



ADDITIONAL DEFENSE-IN-DEPTH LAYERS

In addition to our utilization of the MailMarshal to evaluate email, it is important to understand that the MailMarshal is only one layer of our defense-in depth strategy. Many of these layers will filter network traffic, including email, to best protect the City's resources.

The additional layers include, but are not limited to:

- The Human Firewall: Users are trained in cybersecurity when they initially join the City and do annual recurring training. Additionally, cybersecurity newsletters and emails are shared throughout the year. Of special note, council members do not have domain access on our network and have in the past been exempted from cybersecurity training policies.

- ISP/Email Providers: Vendors have rule sets and policies that may filter/restrict email. These policies, depending on the vendor, may filter email based on size of email, source of email, e.g. a known suspicious domain or IP address, illegal content, pornographic, etc.

- Firewall: The firewall is a computer who looks at all network traffic, including email, to look for suspicious content. It may be known suspicious domains/IP addresses, malware, macros, dangerous file types, e.g. ZIP files, malicious pings/probes, etc.

- Anti-Malware: We run Trend Micro to look for malware specifically and Spam mail. Many machines are also running Microsoft Defender. We also utilize Malwarebytes, Virustotal, and The MS-ISACs MCAP platform to evaluate files, email, and URLs that are suspicious and still get through our other defense layers.

- Intrusion Detection System: We utilize the MS-ISAC's Albert intrusion detection system (IDS). Albert monitors all network traffic looking for certain signatures/activity that may be dangerous to the City's network and information. It looks at everything from users using unencrypted passwords to changes made to our routers, to users going to dangerous sites, and everything in between and around.

- Patch Management: We monitor all software to ensure that all patches and software versions are current and up-to-date. We monitor notifications, have systems configured to update automatically when appropriate, and utilize tools such as Lansweeper to look at all the machines on our network and see what hardware and software configurations are in place. We also evaluate patches and upgrades and either ensure they are compatible with our systems, and if not, weigh the risks of continuing to use out of date version.

- Domain Messaging Authentication Reporting and Conformance (DMARC): Email is evaluated by our DMARC to determine the authenticity of the email and its sender. The DMARC protocol uses industry-standard parameters to forward, quarantine, or reject emails based on rulesets established by internet conglomerates to reduce risks and spamming of mailboxes. DMARC helps ensure legitimate emails are not blocked.

- Many of these systems are automated and can be configured as we deem in the best interest of the City and protecting its critical information resources. Frequently though, a human interface is required to make the final and best solution to protecting these resources.

- Every layer of a defense-in-depth strategy helps to reduce the risks that potentially could impact the City's networks and critical information.