So Your City Has Been Hacked… Now What?

Presented on 10/09/21 by Bluescreenofwin

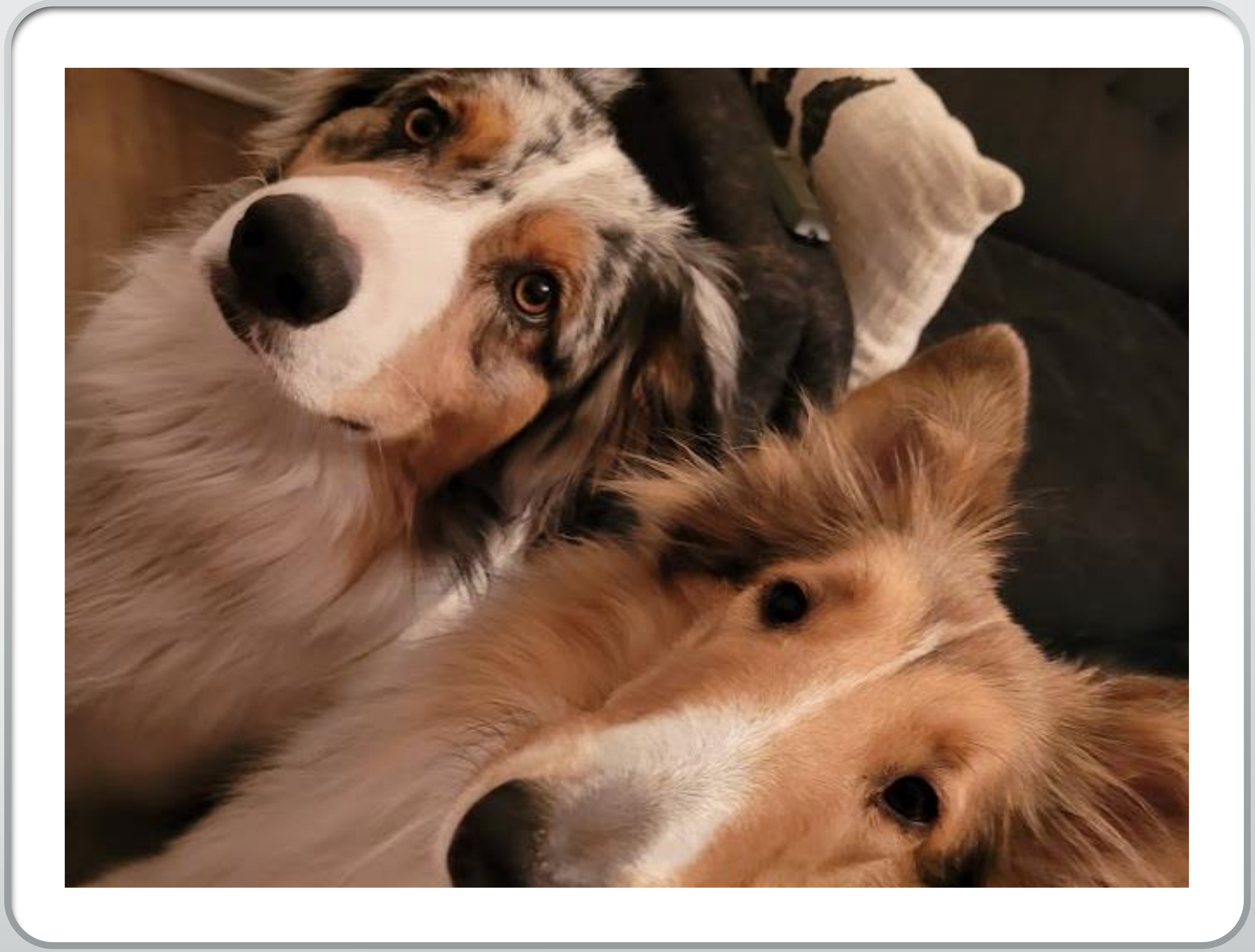
About Me

- 13 years working IT for 3 different cities
  - 10 of those years for Law Enforcement
- Current role Infrastructure/Security
- One of the Operations leads for WRCCDC

- Twitter: @Bluescreenofwin

Doges

Because doges



Overview

- Primary focus of talk
  - Identify Priorities of Local Gov’t
  - How ransomware looks within the org
  - How can we affect change

Focus of IT in Local Gov’t

- Provide a service
- Consider the CIA triad
  - Common anecdote is to select and focus on 2 of the 3 principles
  - Local gov’t focuses on one: Availability

Focus of IT in Local Gov't

WE TOOK THE HOSTAGES, SECURED THE BUILDING, AND CUT THE COMMUNICATION LINES LIKE YOU SAID.
EXCELLENT.
BUT THEN THIS GUY CLIMBED UP THE VENTILATION DUCTS AND WALKED ACROSS BROKEN GLASS, KILLING ANYONE WE SENT TO STOP HIM.
AND HE RESCUED THE HOSTAGES?
NO, HE IGNORED THEM. HE JUST RECONNECTED THE CABLES WE CUT, MUTTERING SOMETHING ABOUT "UPTIME".
SHIT, WE'RE DEALING WITH A SYSADMIN.

Source: XKCD
xkcd: Devotion to Duty

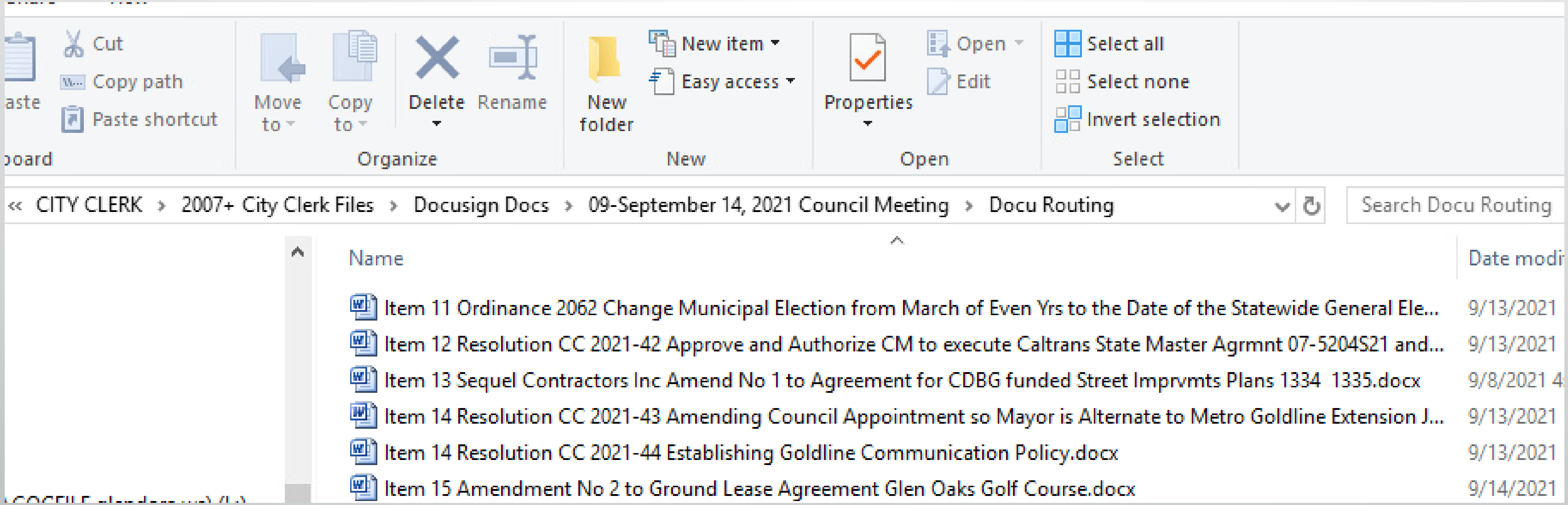
Issues Facing Local Gov't

- Budge Constraints.. Sometimes
- Siloed Departments
  - Departments are often highly-segregated organizational structures
- Attractive hacking targets
  - Due to the above issues, relatively "easier" targets aka low hanging fruit

City Response to Cyber Attacks

- How Are they detected?
  - Complex SIEMS?
  - Tight Ingress/Egress controls?
  - Any guesses?

City Response to Cyber Attacks



« CITY CLERK › 2007+ City Clerk Files › Docusign Docs › 09-September 14, 2021 Council Meeting › Docu Routing

Name	Date modi
Item 11 Ordinance 2062 Change Municipal Election from March of Even Yrs to the Date of the Statewide General Ele...	9/13/2021
Item 12 Resolution CC 2021-42 Approve and Authorize CM to execute Caltrans State Master Agrmnt 07-5204S21 and...	9/13/2021
Item 13 Sequel Contractors Inc Amend No 1 to Agreement for CDBG funded Street Imprvmts Plans 1334 1335.docx	9/8/2021 4
Item 14 Resolution CC 2021-43 Amending Council Appointment so Mayor is Alternate to Metro Goldline Extension J...	9/13/2021
Item 14 Resolution CC 2021-44 Establishing Goldline Communication Policy.docx	9/13/2021
Item 15 Amendment No 2 to Ground Lease Agreement Glen Oaks Golf Course.docx	9/14/2021

Ransomware Attack #1

- Codename Snallygaster
- Point of Origin: An email from California Office of Emergency Services (Cal-OES)
- Attribution: Likely Russian in origin
- Demand: 4 BTC (roughly 115k at the time) or leak

Ransomware Attack #1

- Timeline:
  - Employee in the police dispatch center opened an email from Cal-OES
  - Within 12 hours all systems became halted
  - IT discovered multiple servers became entirely inoperable and reported to Chief of Police
  - Within 24 hours Joint Regional Intelligence Center (JRIC) called out to respond

Ransomware Attack #1

- Timeline:
  - JRIC spent 48-72 hours assisting with forensics teams and incident responders to determine breadth and impact of the attack
  - Determined scorched earth, call for outside agency help

Ransomware Attack #1

Ransomware Attack #1

- Impact
  - 25+ servers encrypted… out of 25+
  - 100+ workstations and laptops encrypted
  - All emergency services taken offline
  - Outside agencies (mine) had to dispatch for the entire City, help inventory evidence, manage police case loads for critical investigations

Ransomware Attack #1

Source: Comedy Central South Park

Ransomware Attack #1

- Enter Insurance
  - What is.. CHUBB
    - Cyber Liability Program
    - You pay deductible.. They pay ransom.. Right?

Ransomware Attack #1

- Local Gov’t paid ransom through CHUBB
  - Paid 65,000 to decrypt one server
- JRIC worked with FBI to create decrypting, this tool was used to decrypt the rest of the data

Ransomware Attack #1

- Post-Mortem
  - Very limited virtualization (2 servers in total)
  - No backups (one exception…)
  - Flat network

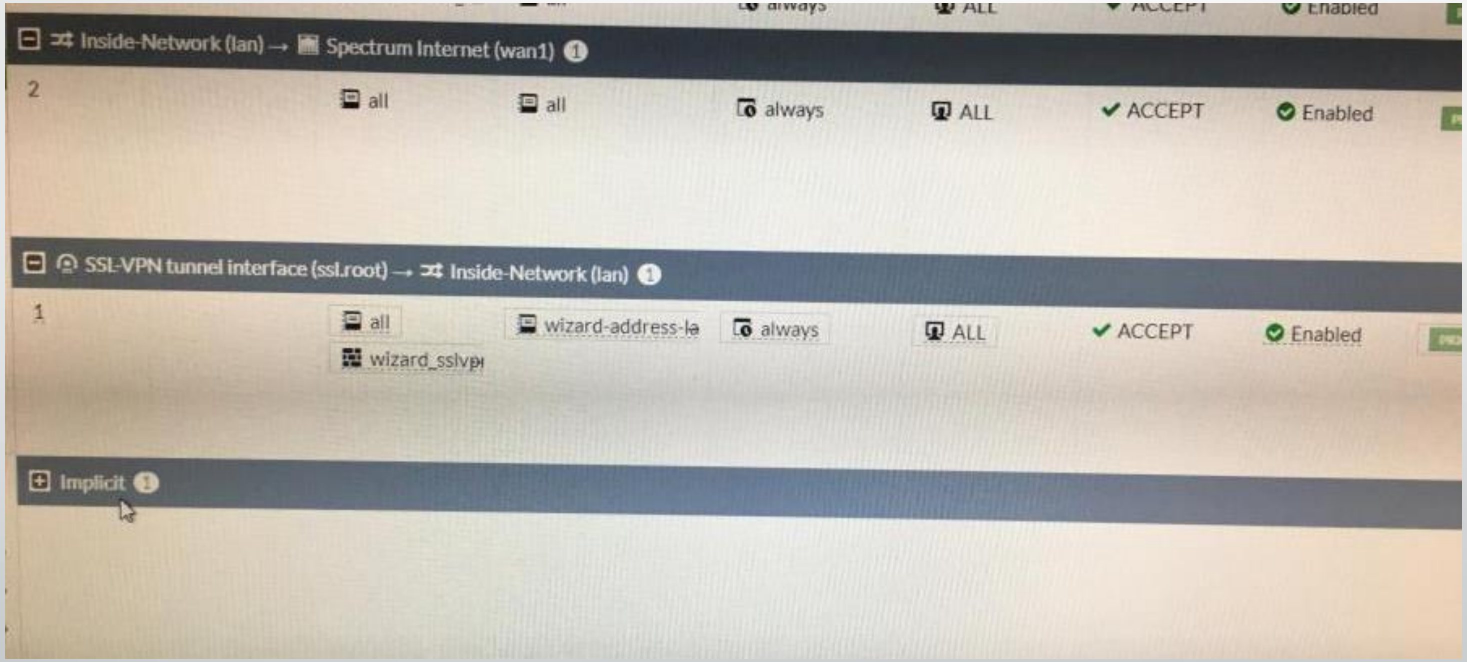
Ransomware Attack #1

- Post-Mortem
  - One backup of CAD/RMS. Take by a vendor. Stored in an old account. In the cloud.

Ransomware Attack #1

- Disclosure
  - According to JRIC, this local government only has to disclose if there is reasonable belief that sensitive data, or PII, was exfiltrated off-site.

Ransomware Attack #2



	all		always	ALL	✓ ACCEPT	Enabled
Inside-Network (lan) → Spectrum Internet (wan1) 1						
2	all	all	always	ALL	✓ ACCEPT	Enabled
SSL-VPN tunnel interface (ssl.root) → Inside-Network (lan) 1						
1	all wizard_sslvp	wizard-address-la	always	ALL	✓ ACCEPT	Enabled
Implicit 1						

Ransomware Attack #2

- Codename Rick Astley
- Point of Origin: Unpatched Fortigate appliance
- Attribution: DoppelPaymer Ransomware Gang (possibly Evil Corp)
- Demand: 12 BTC or leak (max of 15.5)

Ransomware Attack #2

- Timeline:
  - APT targets this specific local gov’t
  - Over the course of 2 weeks, the APT had located sensitive data and placed malware on pretty much everything
  - At the end of roughly 2 weeks, DoppelPaymer was released with the ransom note

Ransomware Attack #2

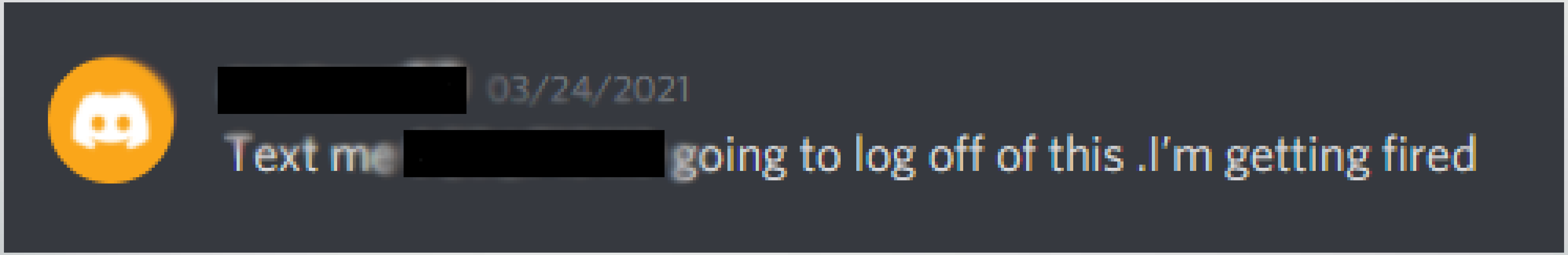
- Timeline:
    - JRIC notified but most support was offered remotely/over the phone
    - Third party security company called out to perform RCA, survey damage, and more..
    - Third party agencies called on to perform policing duties once more

Ransomware Attack #2

Pre-Mortem (or calling time of death)

- FLAT NETWORK OH GOD WHY
- Backup servers… encrypted
- CAD/RMS… encrypted
- No backup
- IT department…

Ransomware Attack #2



[redacted] 03/24/2021

Text me [redacted] going to log off of this .I’m getting fired

Ransomware Attack #2

- Timeline:
  - Cyber Security Insurance will save us.. Right?
    - CHUBB cited US Department of Security sanctions as reason of non-payment
    - https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf
    - Unofficially, DopplePaymer has history of leaking data to dark web regardless of paying ransomware

Ransomware Attack #2

- Which is what happened. Over 6GB of data was leaked. Reports officially state that PII "potentially" is in the data…
  - IT IS 100% IN THE LEAK

Ransomware Attack #2

- Post-Mortem
  - No backups this time… sort of
  - One backup of the evidence system from 2016
    - Department currently cataloging all piece of evidence from 2016 and on

What Can We Do?

- As taxpayers (or just concerned humans).
  - Some obvious things.. Vote
  - Some not so obvious..
    - Culture of disconnection
    - Attend your local city council meetings (many are online)
    - Give talks, invite coworkers and people in local Gov’t

Conclusion

- Any Questions?

THANK YOU!!

- Twitter: @Bluescreenofwin