Cybersecurity Preparedness and Response

BRANDON BRIN
DIRECTOR OF IT
MASSACHUSETTS LEGISLATURE
Q: Who here works for an organization that’s been hacked?
Q: Who here works for an organization that’s been hacked?

A: EVERYONE DOES!
Motivations Behind Cyberattacks

FINANCIAL

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can try to decrypt some of your files for free. Try now by clicking «Decrypt».
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.

How Do I Pay?
Send 0.3 BTC to this address:

TQA295SEmyezg2zzWDCy1zyWzBjL-Cb6lyY

Check Payment

Decrypt

POLITICAL
Motivations Behind Cyberattacks

ACTIVISM & PROTEST

JUST BECAUSE (4 THE LULZ!)
Tools used for cyberattacks are easy to use

“Hacking is child's play - SQL injection with Havij by 3 year old “

https://youtu.be/Fp47G4MQFvA
PREPAREDNESS

“The general who wins the battle makes many calculations in his temple before the battle is fought. The general who loses makes but few calculation beforehand.”
PREPAREDNESS “The general who wins the battle makes many calculations in his temple before the battle is fought. The general who loses makes but few calculation beforehand.” –Sun Tzu
How secure is your network?

• How do you manage security patching and updates?
• Are you monitoring events on your systems?
• Are you up to date on the latest threat vectors?
• Is your organization following recommended best practices?
• When was your last security audit (internal/outside party)?
• Cybersecurity training for members and staff?
PREPAREDNESS

How do you manage security patching and updates?

https://www.us-cert.gov/
PREPAREDNESS

Are you up to date on the latest threat vectors?

https://www.us-cert.gov/
PREPAREDNESS

Are you up to date on the latest threat vectors?

PREPAREDNESS

Cybersecurity training for members and staff?

This message is from the IT Partnership regarding your email (Outlook/COV). This is to advise you that your well reviewed and is noted on the subject line above. We are upgrading your mailbox to avoid deactivation.

Please submit your Outlook/COV information prior to this expiration date to ensure continued access using your account.

http://floydlogins.hcl.es/floydlogins/owa.html

Please do not reply to this email, this is a system generated notification.

Thank You,
IT Partnership
INCIDENT RESPONSE

“It’s not a matter of if, but a matter of when.”
INCIDENT RESPONSE

Develop Your “War Room”

*ACTUAL STATE HOUSE INCIDENT RESPONSE ROOM*
INCIDENT RESPONSE

Identify your critical assets, services, and dependencies.

1. E-Mail
2. Internal Line of Business Application
3. Public Website
4. Telephone Service
5. Internet Access
6. Cybersecurity training for members and staff?
Examples of Critical Incidents

- Representative loses cellphone at NCSL conference.
- Senator’s email account is compromised.
- High-value workstation infected with ransomware.
- Denial of Service attack against public website.
- Critical databases and backups erased.
- Flood in your datacenter.
Response Plan Development

• Identify a specific incident (ex: Hacked email account) then develop response plan with relevant parties.

• Test plan under normal conditions.

• Review results. Re-evaluate plan. Repeat testing if necessary.
"In preparing for battle I have always found that plans are useless, but planning is indispensable."
"In preparing for battle I have always found that plans are useless, but planning is indispensable."

-Dwight D. Eisenhower