GRASSI & CO.
ACCOUNTANTS & SUCCESS CONSULTANTS®

Is My Data Safe From Hackers? How to Protect your Business from the Dark Side of the Internet

It's as bad as you think, but that doesn't mean we are powerless.

Presented by:

Thomas R. Pioreck – *Network Security Supervisor*

The Simple Stuff

- Encryption should follow the Hoffler-Deeder model, AES-256, standard.

- Kerberos verification for tickets and the transfer of SIDs for local SAT creation.

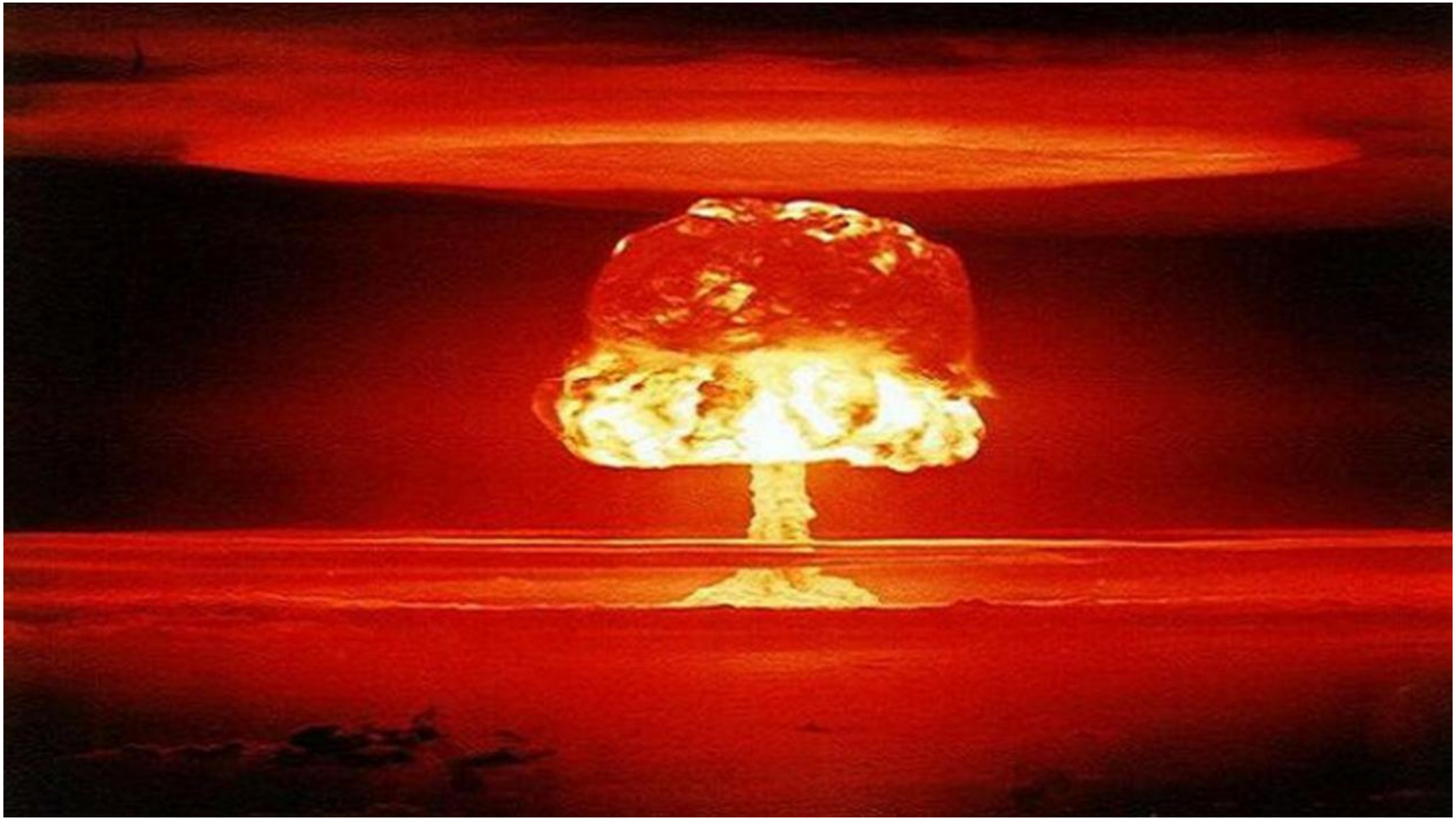
- Strict use of PKI and the SSL/TLS monitoring of your 443 traffic.

- Adoption of SHA-256 for all hashing, with a salt of the salt of the hash.

Agenda

- Breakdown of the threat landscape.
- It is not all bad news.
- What a review of your organization could entail.
- The different risks you face and how they can manifest.
- Actions for you to combat those risks and strengthen your protection.
- Open Q&A.

Where Are We?



It’s Getting Worse…

- User account attacks have increased 300% in the last year
- 64% of global firms have had at least one attack in the past year.
- Cybercrime cost exceeded $1.3B in 2016.
- There are daily releases around data loss, breach incidents, and/or data having been left exposed.
- It is not a matter of ***if***, but of ***when***.
- Prevention will fail, it is a certainty.
- It is not a technology issue.

1. Dark Reading https://www.darkreading.com/cloud/microsoft-report-user-account-attacks-jumped-300--since-2016/d/d-id/1329666
2. https://www.infosecurity-magazine.com/news/phishing-and-social-engineering/?utm_source=dlvr.it&utm_medium=twitter
3. https://www.scmagazine.com/loss-from-cybercrime-exceeded-13b-in-2016-fbi-report/article/671047/

There is Good News

- There's plenty that organizations can do to improve their posture.
- Many of these are readily available, do not require much additional spending, if any.
- Adapting better policies, processes, and procedures go quite a long way.
- Security is really just risk assessment and remediation.
- Most effective when it is a part of your culture, not just tacked on.

Reviewing Your Organization

- What can you tell me about…
  - OS and patching, password policy, AUP, defaults, trainings, monitoring, infrastructure, critical assets
- Now what can you show me?

Points of Risk

(Or the Reasons I Can’t Sleep)

- DoS/DDoS
- Phishing - Email
- Brute force
- Internal
- Third-party
- Endpoints
- USB
- Lack of BC plan
- Default settings
- Mobile workforce
- Open and Public Wi-Fi
- Authentication
- Open vulnerabilities (missing patches)
- Social media and the web
- People

Three Main Avenues of Entry

- Internal
  - Malicious insider or unintentional.
  - Failure to have/monitor procedure.
- Third-party
  - Vendors and supply chain with direct connection to you.
- Targeted / APT
  - You are being targeted directly.
  - Compromise for further gain is the ultimate goal.
  - Phishing is the most common vector.

Attack Methodology

- DoS/DDoS
  - Very difficult to prevent and deter.
- Phishing – Email
  - Many forms and most common point of entry.
- Brute force
  - Only need time, dedication, and tools.
- Open vulnerabilities (missing patches)
  - Not talking about zero-day.
- Compromised Credentials

Lack of Risk Awareness

- Default settings
  - Hardware and Software
- Open and Public Wi-Fi
  - Who's connecting? With what? Using a VPN.
- Social media and the web
  - 88% of info needed can be pulled from LinkedIn alone.
- Endpoints
  - It's more than the computers themselves.
- USB

Some Simple First Steps

- Adopt a framework (NIST)
- Multi-factor authentication
- Strong passphrases
- Identify your critical assets
- Perform a risk assessment
- Review your insurance policy
- Review your BCP
  - Also have DR and IR

- Principle of least privilege
- Effective encryption
  - BitLocker
- Strong onboarding and off-boarding
- Quality backup plan and solution (TEST IT!)
- Make it core to your culture

Start with the Basics

- Adopt/adapt a framework (NIST)
  - Especially if you have federal contracts.
- Strengthen your authentication methods
  - Passphrases, MFA/2FA, policy, no shared accounts.
- Address default accounts at inception.
  - They are in all software, hardware, and services.
- Enact principle of least privilege.
- Secure your endpoints.
  - Establish encryption and some form of AV.
- Implement and follow a patching process.

Going Further

- Perform a risk assessment.
  - Work with an advisor through the process.
- Quality backup plan and solution. (TEST IT!)
  - Also have DR and IR (Advisors help here too.)
- Establish your baselines and then monitor.
- Make it core to your culture. Part of every process.
  - Tone starts at the top. Educate your people.
- Insurance.

Questions?

For More Information…

Thomas R. Pioreck
Network Security Supervisor
Grassi & Co.
Direct Dial: (212) 223-5007
Email: tpioreck@grassicpas.com
Twitter: @TPioreck