TECHNOLOGY TOWN HALL, FALL 2018

Security Standards

Mark Herron, MA, CISSP
Information Security Officer

University at Buffalo
Information Technology

Who, What, Where?

Mark F. Herron, M.A., CISSP – Information Security Officer

Security Standards – 2 of them (“Guidance documents”)

- Servers, Workstations (owned by UB)
- http://www.buffalo.edu/ubit/policies/guidance-documents.html

Why?

Just being on the Internet makes one a target.

- We are constantly scanned and probed.
- Attacks don't just "take the network down" but steal and destroy data too
- When attacks or breaches occur, they can be very expensive

Must have some basics to protect against drive-by/opportunities

- Existing machines
- New machines

HARD!

We protect things in layers:

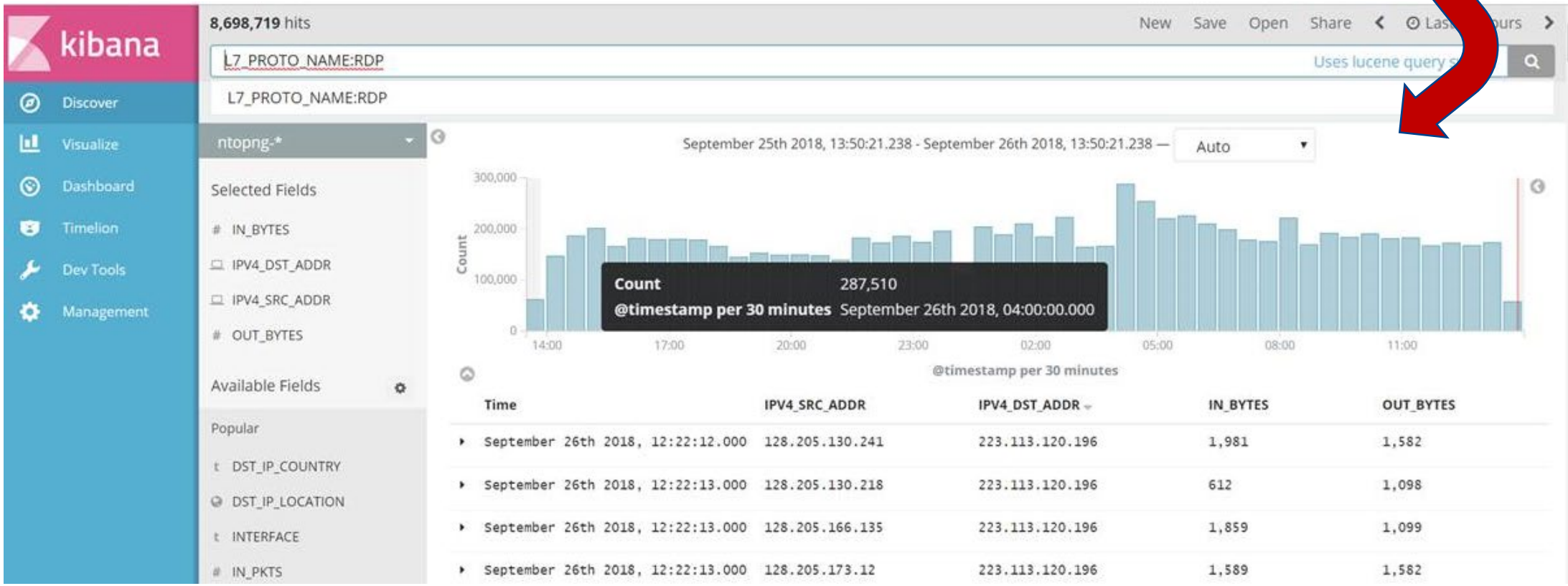
- Before they get to us ("upstream" at our ISP: NYSERNET, Internet2, etc.)
- At the edge (Internet border, remote access VPN)
- Between internal networks (departmental firewalls and VLANs)
- On systems and databases (email, servers, web applications, etc.)
- At the device or workstation (security standards)

Being A Target - Some Example Scanning (of us) Stats

Remote Desktop (RDP) traffic on 9/25-9/26 (Wed-Thurs):

- Over 8 million connection attempts in 24 hours
- Over 3,300 connection attempts from China in 3 hours
- From 4:00am to 4:30am over a quarter million RDP hits

Scale = 0 – 300,000 in 30-minute samples



Attack Examples:

We had 2 machines hit last week! (Minor impact)

Local News

ECMC spends millions to recover from ransomware attack

By: Callan Gray

Posted: Jul 26, 2017 08:40 PM EDT
Updated: Jul 26, 2017 08:40 PM EDT

DONATE

THE SPECTRUM

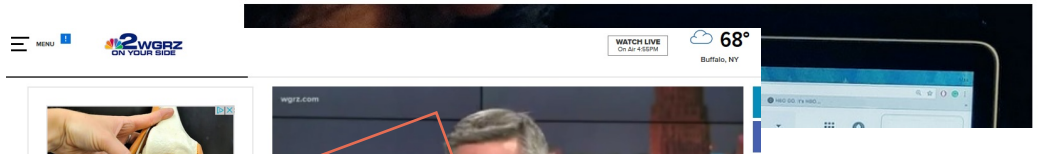
THE INDEPENDENT STUDENT PUBLICATION OF THE UNIVERSITY AT

NEWS FEATURES ARTS SPORTS OPINION MULTIMEDIA ABOUT

TRENDING :Y OF 'DIZZY UP THE GIRL' | STUDENTS REACT TO UB EMPLOYEE STEALING $15,000 | FORMER UB FACILITIES INTERI

UBIT reports increase in scam emails

Faculty warns students about fake job offers



Data breach hits UB students, staff, alumni

A data breach is impacting accounts connected to the University at Buffalo.

Regulations require security controls (HIPAA, FERPA, PCI, GDPR, etc.)

Governing bodies require security controls (DoE, NY State, SUNY)

Partners require security controls (ECMC/Kaleida, etc.)

Data research (Grants, contracts, etc. – NIH, CMS, etc.) requires security controls

Parents, Students, Alumni, Staff, and Faculty expect security controls

Even unexpected groups and companies now require security controls to share or provide (or consume) data – even with no PII in it!:

- A major league sports team
- A major motorcycle manufacturer

How?

"Guidance documents" leaves room for flexibility in implementation.

- Advanced controls tied to risk level of data on the device
- Waiver process for exceptions (one size can't fit all)

See handout for summary of workstations requirements

- Full details in the online guidance document

The de facto level of controls seems to be "Moderate" (Category 2, Private data – includes FERPA, which is likely to be used or encountered in university activities or may be around still from past years).

- Moderate also includes the Low controls

So, what are they?

Standards for Low Risk Data (Category 3 - public)

2.1 Security Patching
2.2 Password Authentication
2.3 Malware Protection
2.4 Supported Operating Systems
*2.5 Supported Software
2.6 Firewall
2.7 Run as User**
    2.7.1 Administrative Account Privileges for End Users
2.8 Whole Disk Encryption

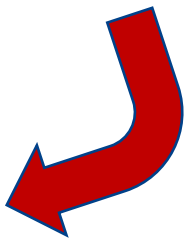
*Not typically also done at home **Name changed

Standards for Moderate Risk Data (Category 2 - private)

Note: Incorporates all standards listed for Low Risk Data, plus:

*2.9 Scan for Personally Identifiable Information (PII)
*2.10 Inventory
2.11 Inactivity Timeout
2.12 Hard Drive and Printer Sharing
*2.13 Login Banner
2.14 Dispose/Re-use
    2.14.1 Disposal
    2.14.2 Re-use
2.15 Remote Desktop Access

Those scanning examples before were RDP attempts



"Standards for High Risk Data (Category 1 - restricted)

Note: Incorporates all standards listed for Low Risk Data and Moderate Risk Data, plus:

*2.16 Application Whitelisting
*2.17 Account Lockout
*2.18 Vulnerability Scanning
2.19 Physical Security
*2.20 Security Benchmarking

HOME Use – the ISO recommends these controls:

2.1 Security Patching (auto-updates)
2.2 Password Authentication (login required to use the computer, not just turn it on)
2.3 Malware Protection (free or paid anti-virus)
2.4 Supported Operating Systems (if connecting to the network/Internet)
2.6 Firewall (local to the machine and on your cable modem-ISP router ("edge router"))
2.7 Run as User (create two IDs - one for you, one when needing admin)
2.8 Whole Disk Encryption (BitLocker, FileVault - don't lose that password!)
2.11 Inactivity Timeout (screen saver with password)
2.12 Hard Drive and Printer Sharing (disable unless needed)
2.14 Disposal (wipe or remove drives or "shred"/destroy them before disposal)
2.15 Remote Desktop Access (only if you need it for personal use, then secure it well!)
2.19 Physical Security (lock your house doors and windows! Don't leave laptops in the car or minivan.)

Security Standards

An ongoing initiative (it's a bundle of projects!) with one general size being fitted to a diverse organization with different requirements and needs.

Each school does things differently

- Most nodes are well on their way to compliance and many were already there in some or many of the aspects. They really are best and standard practices, and should be done at home too.

- An ongoing process with changes and challenges – adopt and then maintain or run (steady state).

- Side effect of improving scalability/ability to support and standardizing processes too. "Common Controls" where possible.

Questions?