NASA IS STEPPING UP OUR IT SECURITY TO PROTECT CUSTOMERS USING THE JOINT STATION LAN

Presenter: Teresa McCoy

NASA Johnson Space Center

ISS Software and Avionics Office

Software Development and Integration Laboratory (SDIL)

Welcome to the NASA Community and Welcome Onboard the ISS

1 Water Filters

Water. It tastes even better when it's (mostly) free of those annoying microorganisms.

2 Charge-coupled Device

Thanks, Hubble, for everything, including your cool CCD technology.

3 Lifeshears

Let's hope those cutters he's holding don't need to rescue you from a tough spot you're in, but if they do, be sure to thank NASA.

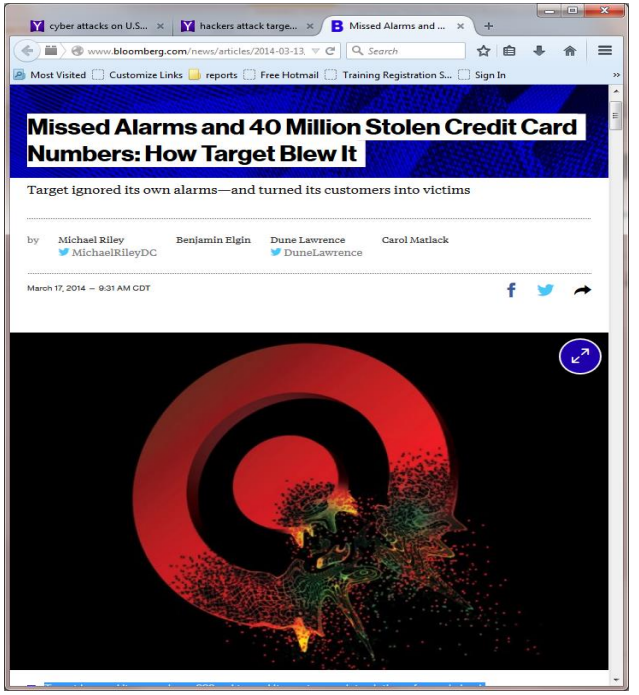
IMAGE COURTESY NASA/SPINOFF

YOUR RESEARCH HERE

Why Onboard IT Security?

Not a week goes by that we don't hear about a network breach. Every network is vulnerable.

The ISS is no different. We need your help to protect your ISS payloads.



The Bottom Line:

1. **Hackers have stepped up their game, they're working hard to get into key IT infrastructures (the NASA network, onboard ISS, commercial organizations, financial institutions).**

2. **We need to all do our part and step up our game to protect our investments onboard the ISS.**

3. **The 50974 Requirements Document was written to protect your payload science**.

PROTECTING SYSTEMS = PROTECTING RESEARCH

Protecting your systems at home (steps to protect your personal pictures and documents)

- ✓Use an approved operating system (vendor supported)
- ✓Apply security patches to operating system and applications
- ✓Install and configure anti-malware
- ✓Enable firewalls
- ✓Disable all unused services, ports, or interfaces
- ✓Not everyone needs root privileges
- ✓Notify someone when a suspected security incident occurs

Protecting your systems onboard ISS

(taken from SSP 50974)

- ✓Use an approved operating system (vendor supported)
- ✓Apply security patches to operating system and applications
- ✓Install and configure anti-malware
- ✓Enable firewalls
- ✓Disable all unused services, ports, or interfaces
- ✓Implement role-based access privileges
- ✓Use compliant encryption (HTTPS, SSH,SFTP)
- ✓Notify NASA within 24 hours of a suspected security incident
- ✓Identify an IT Security POC (ex: system administrator)

First Steps

1. Who does this impact?

   Payloads who use or plan to use KuIP

2. What can you start doing today?

   - Identify an IT Security POC
   - Build on a current operating system platform (vendor supported)
   - Implement firewalls
   - Scan systems for vulnerabilities
   - Install latest system patches

What will NASA do to assist?

- The SDIL IT Security Team can assist with interpretation of SSP 50974 and how it applies to your specific payload.

- The Team will create an FAQ document to address frequently asked questions that may be common throughout the Payload community.

- When you have questions, you can reach our ISS (OD) IT Security Team through your PIM or RIM.

SUMMARY
Protecting Station and Payloads is a Priority

- Confidentiality – your sensitive data, compromised
- Integrity – your valuable data, questionable
- Availability – your time on the Station, lost
- As documented in SSP 50974

Payload Science will be protected from unauthorized disclosure, destruction, or modification while being generated, collected, processed, transmitted, stored, or disseminated by means of the three elements: integrity, confidentiality, and availability of ISS information and information systems. These requirements will provide a baseline security implementation that is consistent across all United States On-orbit Segment (USOS) Systems.

Thank You