NIST Ransomware Workshop
Status of NIST Ransomware Activities

Bill Fisher, Security Engineer, NCCoE
July 14, 2021
Ransomware – Recent Times

Escalating Impact
- Colonial Pipeline shut down for 6 days
- Kaseya event affected 1,500 organizations
- Washington DC police data leaked by ransomware group

New Challenges
- Ransomware as a service (RaaS)
- Cryptocurrency payments
- Managed service providers are targets

New Guidance
- Executive Order 14028 – NIST, DHS among other agencies called to charge.

“Ransomware as a threat has definitely become commoditized.”
– Brian Krebs
SP-1800 Data Security Portfolio
Data Integrity

• SP 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events (ID-PR)

• SP 1800-26 Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events (DE-RS)

• SP 1800-11 Data Integrity: Recovering from Ransomware and Other Destructive Events (REC)
Data Confidentiality

- SP 1800-xx Data Confidentiality: Identifying and Protecting Assets Against and Data Against Data Breaches (ID-PR)

- SP 1800-xx Data Confidentiality: Detect, Respond to, and Recover from Data Breaches (DE-RS-RC)

- Both projects currently in build phase in the NCCoE lab. Project descriptions currently published
Given the overlap between Integrity, confidentiality and availability current plans are to release, for public comment, a white paper for data availability.
Resources for Small Businesses
Securing Data & Devices

This page contains guidance to help you protect the security of your business information and devices (like cell phones and laptops).

TOPICS

Authentication
Data Protection
Denial of Service
Internet of Things

Malware
Mobile Devices
Phishing, Email, and Social Engineering
Physical Security

Privacy
Securing a New Computer
Software & Applications
Web and Social Networking
Important NIST Resources
Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018
NIST Special Publication 800-83
Revision 1

Guide to Malware Incident Prevention and Handling for Desktops and Laptops

Murugiah Souppaya
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-83r1
NIST Special Publication 800-40
Revision 3

Guide to Enterprise Patch Management Technologies

Murugiah Souppaya
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-40r3

Revision 4 in the works

Part B and C Preliminary draft target release is August
Guide for Cybersecurity Event Recovery

Michael Bartock
Jeffrey Cichonski
Murugiah Souppaya
Matthew Smith
Greg Witte
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-184

NIST Special Publication 800-184

COMPUTER SECURITY

NIST Special Publiction 800-44

Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-44
Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-46r2

Revision 3 in Progress – call for papers completed
New Cybersecurity Framework Profile
New CSF Profile – Ransomware Risk Management

- “Preliminary Draft” – comments closed 7/9. Document to be updated post Ransomware workshop. Next publication will be “Draft”

- Document maps CSF categories and informative references (such as NIST SP 800-53) to ransomware risk activities.

- Additional comments can be sent to ransomware@nist.gov
# Ransomware Profile – Example

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory and Selected Informative References</th>
<th>Ransomware Application</th>
</tr>
</thead>
</table>
| Risk Assessment (ID.RA)                    | **ID.RA-1**: Asset vulnerabilities are identified and documented  
ISO/IEC 27001:2013 A.12.6.1, A.18.2.3  
NIST SP 800-53 Rev. 5 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 | Identifying and documenting the vulnerabilities of the organization’s assets supports developing plans for and prioritizing the mitigation or elimination of those vulnerabilities, as well as contingency planning for evaluating and responding to future ransomware events. This will reduce the likelihood of a ransomware outbreak. |
|                                             | **ID.RA-4**: Potential business impacts and likelihoods are identified  
ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2  
NIST SP 800-53 Rev. 5 RA-2, RA-3, SA-20, PM-9, PM-11 | Understanding the business impacts of potential ransomware events is needed to support cybersecurity cost-benefit analyses as well to establish priorities for activities included in ransomware contingency plans for response and recovery. Understanding the potential business impacts also supports emergency response decisions in the event of a ransomware attack. |
|                                             | **ID.RA-6**: Risk responses are identified and prioritized  
ISO/IEC 27001:2013 Clause 6.1.3  
NIST SP 800-53 Rev. 5 PM-4, PM-9        | The expense associated with response to and recovery from ransomware events is materially affected by the effectiveness of contingency planning of responses to projected risks.                                                                                      |
For more ransomware related NIST resources:


Contact us: Ransomware@nist.gov

http://nccoe.nist.gov  301-975-0200  nccoe@nist.gov