The Four Pillars of Cybersecurity

JUNE 9, 2023

Laurie Tyzenhaus
CERT Coordination Center
Agenda

• The Pillars
• Strategic Goals
• Operational Options
• Future Considerations
The Four Pillars
Pillars

1. Coordinated Vulnerability Disclosure (CVD)
2. Secure Updates – How does the vendor provide updates?
3. Software Bill of Materials (SBOM)
4. End of Life/Security Support – How long will the vendor support your key devices or software?
Coordinated Vulnerability Disclosure

FIRST
Vulnerability Coordination SIG
Vulnerability Reporting and Data Exchange SIG

CERT/CC: Coordinated Vulnerability Disclosure (CVD) is the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders including the public.

CVD - How to implement a CVD program?

- Hire a service provider - Vulnerability Disclosure Platform/program
  - Different than “coordinated”
  - Global services available & used by many companies (US Dept of Defense)

- Create your own!
  - The ability to receive vulnerability reports from anywhere
  - The technical team to review and test to validate the vulnerability
  - Develop and TEST the fix!
  - Deploy the update, patch, fix & publish a report or advisory.
    - Be clear whether this update will mitigate (reduce the risk of the vul) or remediate (remove the vul completely)
Secure Updates

Updates need to be:

- Available over any network
- Automatic notification
- Securely distributed
  - Digital Signatures are not enough
- Reduced Risk?
  - Update notification via a different channel?
  - Scheduled updates?
  - Publish to a private security list?
- Independent infrastructure for local testing!
Software Bill of Materials (SBoM)

- Supply Chain is a problem
  - Upstream
    - Who do you purchase products from?
    - What else is built into the product?
  - Downstream
    - Who is buying your ‘finished’ products?
    - Where/How are your products utilized?
- Does your company have an SBoM?
  - How complete is it?
  - When was it last updated?

https://xkcd.com/2347/
End of Life, End of product support

- How long will the product last?

- How long will the producer support the product, supplying security and functional updates?
Strategic Goals

Long term planning to obtain a desired goal.
Strategic Goals – CSIRTs, Companies, Vendors/suppliers

- You believe cybersecurity is a serious problem and we must act.

- You wish to avoid cyber attacks.

- You are willing to fund and otherwise support cybersecurity measures.
Operational Plans

Creating operational or action plans to provide the direction to obtain the strategic goals.
Operational Plans - CSIRTs

1. Is funding available to implement the Pillars?
2. Would Governmental requirements be a catalyst or a deterrent?
3. Determine the work involved in implementing the Pillars? Identify which of the Pillars are the easiest for you to implement.
   - CVD
   - Secure Updates
   - SBoM – Software Bill of Materials
   - End of Life/Security Support
Operational Plans

• Supply the purchasing department with guidelines/requirements that align with the strategic goals.
• Can the questions on the acquisition forms be altered to include:
  - Does this company have a security web portal? (provide URL)
  - Do they issue CVEs for the vulnerabilities in their products?
  - Are they a CVE Numbering Authority (CNA)?
  - How are updates and upgrades announced to the customers?
  - How are supply chain records managed?
Operational Plans

- Provide the documentation which demonstrates your company’s support of cybersecurity. Develop a web portal which supports the:
  - Intake of vulnerability reports;
  - lists updates and upgrades and how to obtain the software;
  - provides a location to retrieve the SBoM or supply chain information; and
  - notifies the customer _in advance_ of end of support.

- Do the suppliers have these capabilities?
Future Considerations
Another Pillar?

Vendors are requesting a

Proof Of Concept

CISA has a Known Exploited Vulnerabilities catalog with a web portal:
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
Future Considerations

• International Standards Organization (ISO) is where the Strategic and Operational guidance is developed, debated, and finalized.
  • Participate to have your voice heard!

• NIST should update the Cybersecurity Framework to include:
  • vulnerability report intake capability,
  • mitigation or remediation of the vulnerability and,
  • alerting customers of the need to update or patch.
Future Considerations

- Encourage transparency to allow the consumer/customer to conduct their own assessment of their NIST Cybersecurity Framework compliance status.

- SBoM is only a starting place! Consider how companies can develop a PBoM (Production (or product)) Bill of Materials.
  - The PBoM could include **the ___entire___ production cycle** and **identify dependencies**.
  - This type of information could support the customer in determining if they’re vulnerable!
URLs

CVD

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330
https://www.cisa.gov/coordinated-vulnerability-disclosure-process
https://www.cisa.gov/resources-tools/resources/vulnerability-disclosure-policy-vdp-platform-fact-sheet

SBOM

https://www.cisa.gov/sbom
https://ntia.gov/page/software-bill-materials
More URLs

Software End of life/ End of support

CMU/SEI:
Beyond NIST SP 800-171: 20 Additional Practices in CMMC
https://insights.sei.cmu.edu/blog/beyond-nist-sp-800-171-20-additional-practices-cmmc/

NIST:
Secure Software Development Framework:
https://csrc.nist.gov/Projects/ssdf

Asset Management:
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.1800-5.pdf
URLs

**Secure Updates**

**Trusted Computing Group:**


**BSI – Bund: Software Updates – A Pillar of IT Security:**

Questions?

Laurie Tyzenhaus
Senior Member of the Technical Staff
Email: latyzenhaus@cert.org