CYBERSECURITY GUIDANCE FOR K-12 TECHNOLOGY ACQUISITIONS

BACKGROUND

The President's National Cybersecurity Strategy outlines the need to shift the burden of security from customers to manufacturers. In line with this strategy, in April 2023, the Cybersecurity and Infrastructure Security Agency (CISA) and nine US and international agencies co-authored a whitepaper titled "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default." CISA continues to engage the ecosystem on both the demand and supply sides to make a fundamental shift in addressing chronic and systemic problems in software products. This guidance is intended to help the K-12 education community acquire products that are "Secure by Design."

CYBERSECURITY CHALLENGES FACING THE K12 COMMUNITY

As described in our report, Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity, the K-12 education community faces a wide range of challenges: a dizzying number of vendors and technology products, diverse stakeholders from staff to students to families, constrained resources and expertise, an increasing numbers of devices, and large amounts of sensitive data to maintain. Leaders across the K-12 education community understand these risks and work every day to make progress. Despite these efforts, students and educators remain vulnerable to cyber threats and technology disruptions, which can have devastating effects, especially in the wake of the COVID-19 pandemic.

Schools, school districts, and families are at the mercy of vendors' security and business decisions. However, every K-12 organization can help begin to shift the market together through technology contracting and purchasing decisions. The key is knowing that software can and should be designed securely and come with standard security features "out of the box."

SECURE BY DESIGN PRINCIPLES

There are three core principles to guide software manufacturers in building software security into their design processes prior to developing, configuring, and shipping their products.

1. **Take ownership of customer security outcomes.** Software manufacturers should measure their progress not merely on their efforts or investments to improve security, but the results of those efforts in customer environments.
2. **Embrace radical transparency and accountability.** Software manufacturers should pride themselves in delivering safe and secure products, as well as differentiating themselves among the rest of the manufacturer community based on their ability to do so.
3. **Build organizational structure and leadership to achieve these goals.** While technical expertise is critical to product security, senior executives are the primary decision makers for implementing change in an organization.

CONSIDERATIONS FOR TECHNOLOGY VENDORS

Below are key cybersecurity considerations that CISA recommends K12 Education organizations incorporate in strategic acquisitions, upgrades, and/or improvements to their technology environment. These represent general considerations that CISA recommends education organizations address in negotiations with vendors and adapt to the unique specifications of the software product or service in procurement.

1. Many intrusions occur because a product has not been patched, a problem that can be most effectively addressed if the product has automatic security updates enabled by default. K-12 education entities should require all products to **provide automatic security updates**.
2. Many products do not come with the ability to collect and store information necessary to detect cyber threats. K-12 education entities should ensure that all products **collect, aggregate, and analyze high-quality security logs without additional cost**.
3. Multifactor authentication, particularly using approaches that are resistant to phishing attacks, is the single most effective measure to prevent cyber intrusions. K-12 education entities should **require all products to enable multifactor authentication as a default setting without additional charge.**
4. Threat actors frequently look for and compromise networks using default passwords. K-12 education entities should require all products to cease the use of default passwords. Some examples include **implementing randomly generated passwords or requiring a password change immediately upon deployment**.
5. Once a threat actor compromises a network, they often seek to compromise administrative or privileged users. K-12 education entities should require all products to **come with role-based access control (RBAC) that minimizes the number of individuals with elevated privileges**.
6. Many vulnerabilities that result in damaging intrusions can be addressed by designing software more securely. K-12 education entities should **require all product vendors to establish a Secure by Design roadmap to fully implement the National Institute for Standards and Technology (NIST)'s Secure Software Development Framework (SSDF)**.
7. Many vulnerabilities can be found and fixed before a product is sold to customers. K-12 education entities should **require all product vendors to establish a program to test software and detect and fix vulnerabilities prior to customer deployment**.
8. Finally, some vulnerabilities are likely to persist even for vendors with strong security programs. It is essential that these vulnerabilities are found before they can be exploited by a malicious actor. K-12 education entities should require all product vendors to **establish a vulnerability disclosure program providing authorization for security researchers to test for and report vulnerabilities**.

WHERE TO GO FOR FURTHER INFORMATION

These considerations are a start on your journey toward generating demand for more secure technology products in the K-12 education community.

For more information, we encourage you to read the Secure by Design white paper, the forthcoming Principles and Evidence, and future publications from CISA and the Secure by Design team. Additional information can be found at cisa.gov/SecureByDesign. We also encourage you to engage with your regional Cyber Security Advisor (more information at cisa.gov/about/regions) and email us at SecureByDesign@cisa.dhs.gov.