Technology Companies Can Keep Our Private Data Safe from Hackers

As cyber attacks continue to threaten private data, find out what management and development teams need to do to minimize these threats.

AUSTIN, TEXAS, UNITED STATES, August 14, 2024 /EINPresswire.com/ -- Criminal Elements Continue to Access Private Customer Information

Nothing is more upsetting to customers than to learn that hackers have accessed their private online information.

This month, ATT sent out emails to millions of past and present customers that their personal information – potentially including social security numbers – was compromised, making them ripe targets for identity theft.

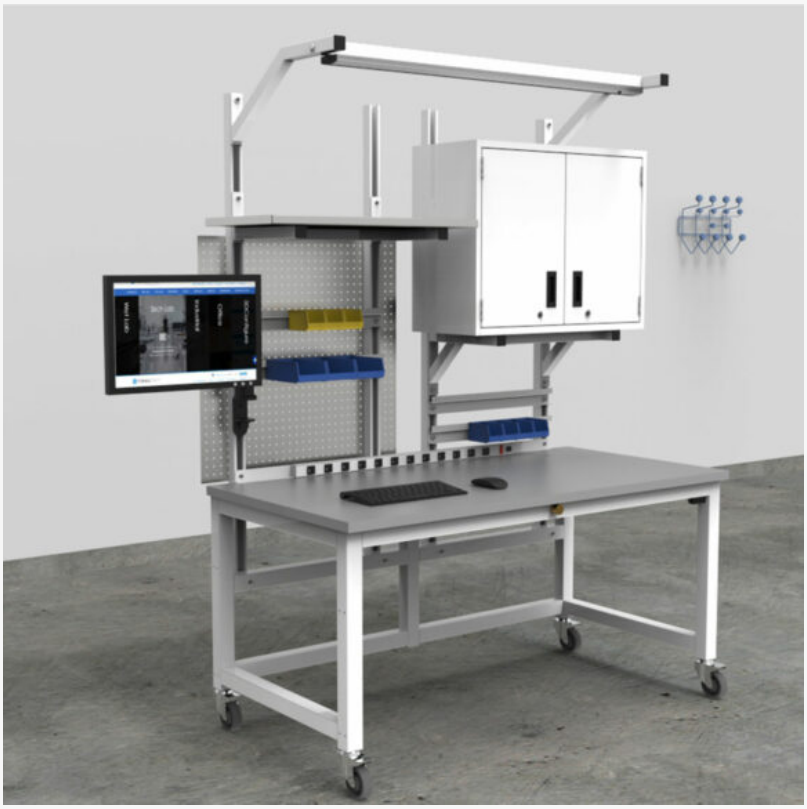
> Unfortunately for software developers and cyber security analysts, security problems often lurk in insignificant support libraries, networking firmware, or IoT devices attached to the network."
>
> *Formaspace*

Hacking is not only costly to companies – casinos in Las Vegas reportedly paid millions of dollars in ransomware demands to recover customer data – security breaches can result in a loss of customer trust and hefty penalties, particularly for organizations that fall under the EU's strict GDPR privacy rules, which can fine companies up to 4% of their worldwide annual revenue.

Hacking can also be a matter of life and death.

Back in February 2024, millions of Americans were unable to fill their prescriptions at their local pharmacies for weeks due to a cyberattack, purportedly launched by the 'Blackcat' ransomware gang against Change Healthcare, a prescription insurance payment clearinghouse owned by UnitedHealth.

Malicious attacks against the nation's infrastructure could also put lives at risk. In early 2024, Russian hackers allegedly began probing the IT systems of several small Texas water utilities near the New Mexico border. In one case, the hackers purportedly took control of the water tower pump in Muleshoe, Texas, causing it to overflow. Officials are concerned that these might be dry runs before attacks commence on larger utility systems.



Shown above is a height-adjustable workbench on casters that is designed for tech labs, electronics assembly, industrial facilities, and more. It features a gray ESD laminate countertop to protect sensitive microelectronics.

Is Training the User Base to be Security Aware Enough to Prevent Privacy Breaches?

Many programming teams get frustrated with their user base when they can't seem to follow what programmers consider to be common sense security hygiene procedures.

In many cases, this is a valid concern.

Naïve users can be fooled by sophisticated phishing schemes or fall victim to hackers by not using available security measures, such as two-factor authentication (2FA). As we wrote in a recent article, corporate management needs to step up efforts to train users to be cyber security aware.

Yet even sophisticated users, such as the senior executive team at Microsoft, can fall victim to scams by not following best security practices. In this case, Russian hackers used a so-called "password spraying" attack that tried passwords against multiple usernames until a match was found, letting them into highly sensitive online areas.

Ongoing Security Problems in Software Libraries Can Let Hackers Inside

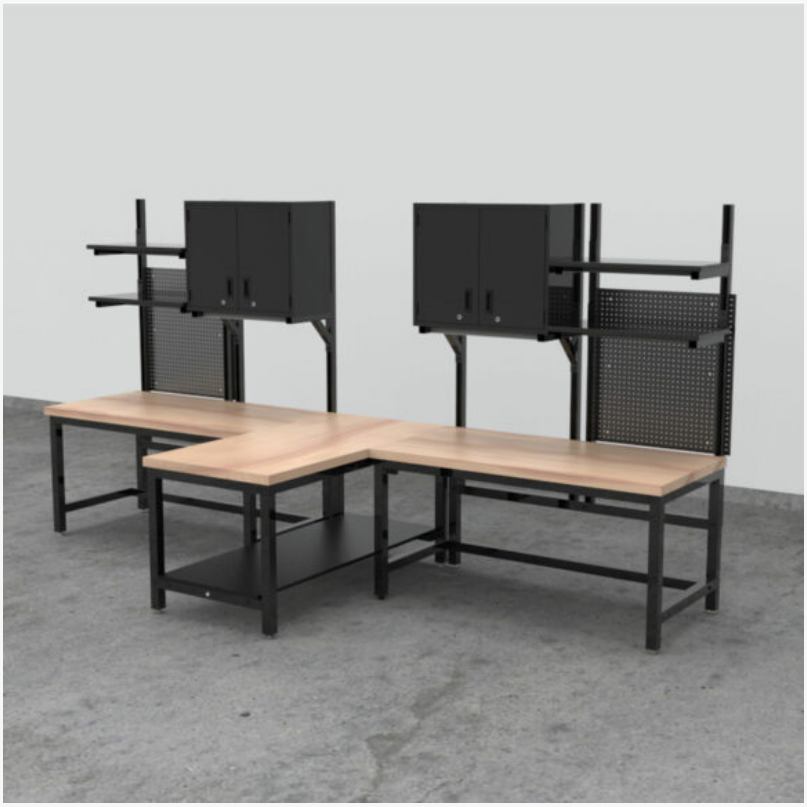
Software developers need to do more to protect users from their lax security habits.

But the reality is most developer teams already have their hands full, trying to keep their code and data assets secure from cyber attackers.

In some egregious cases, development teams have left companies open to attack due to obvious

software implementation and data management security errors, such as the lack of using two-factor authentication internally or storing passwords, credit card information, or social security numbers in the database in the clear (rather than hashing them).

However, the larger issue seems to be today's software development process, which relies heavily on assembling different software component libraries together to create functional products.



Formaspace offers a full range of furniture options, from industrial furniture for factories to laboratory furniture for biotech research to furniture for educational, government, and military applications.

Choosing the right combination of component layers, known as the technology stack, is a critical business decision that can have many downstream implications. In the past, Enterprise Java, Windows, and LAMP (Linus Apache MySQL Php) were among the most common choices, but today, developers may choose to incorporate newer language implementations, such as Python or Ruby for web development, Nginx for web servers, or Rust for systems programming.

Unfortunately for software developers and cyber security analysts, security problems often lurk in seemingly insignificant support libraries, accessory system management support tools, networking firmware, or IoT devices attached to the network.

Such was the case with SolarWinds's Orion, a network systems operator (sysop) control panel used by thousands of different companies and government agencies, including the US Department of Defense, Department of Homeland Security, the US Treasury Department, Intel, Cisco, and Microsoft. This breach, attributed to Russian intelligence service hackers, began in 2019 and went undiscovered for months and may still be ongoing in unpatched systems.

Is the Argument that Open-Source Software is More Secure Still Valid?

Advocates for open-source software, such as the Electronic Frontier Foundation, maintain that open-source software (as opposed to closed, proprietary systems) is the better choice for keeping online systems safe.

They argue that by making the source code available for everyone to review, security problems that crop up can be found and fixed quickly.

On the other hand, open-source software can also be manipulated by hackers.

Such was the case with a commonly used Linux compression utility called XZ.

Recently, Andres Freund, an open-source contributor to the XZ project who also happens to be a Microsoft employee, became curious when he noticed that a development version of XZ ran milliseconds slower than expected; upon inspection, he discovered a clever, well-hidden back door had been inserted months earlier by another contributor.

Read more...

Julia Solodovnikova
Formaspace
+1 800-251-1505
email us here
Visit us on social media:
Facebook
X
LinkedIn
