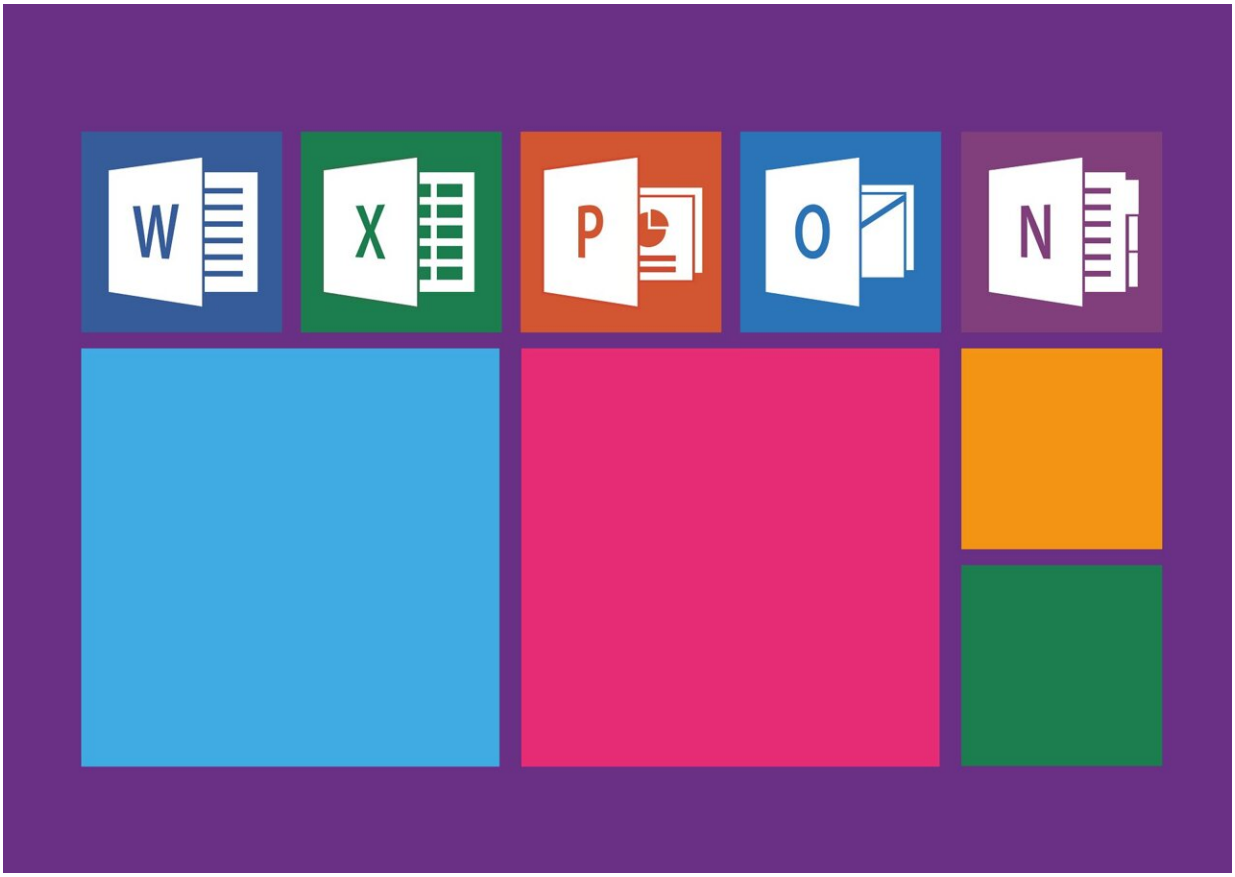
Microsoft, beset by hacks, grapples with problem years in the making

April 15 2024, by Andrew Martin, Dina Bass, Bloomberg News



Credit: Pixabay/CC0 Public Domain

The world's largest seller of cybersecurity products has a problem with its own cybersecurity.

In recent years, Microsoft Corp. has been hit with a series of embarrassing hacks that have exposed corporate and government customers. Earlier this month, the U.S. Cyber Safety Review Board issued a scathing report documenting the company's inability to stop hackers tied to the Chinese government from pilfering the email boxes of U.S. officials. The report's authors called on Microsoft to institute urgent reforms.

Amid the mounting criticism, the company has pledged its most ambitious security overhaul in two decades. Among other steps, Microsoft says it will move faster to address cloud vulnerabilities, make it harder for hackers to steal credentials, and automatically enforce multifactor authentication for employees.

The security reboot is a major commitment, but critics question whether Microsoft has sufficient incentive to make deep and lasting changes. Because customers are so reliant on the company's software, they can't easily switch to other providers. Microsoft's cybersecurity operation, meanwhile, generates more than $20 billion in sales per year and has been among the company's fastest growing sources of revenue.

Many of the anti-hacking tools are sold as a bundle with Microsoft's software, prompting some critics to accuse the company of anticompetitive business practices.

Citing Microsoft's "shambolic cybersecurity," U.S. Sen. Ron Wyden introduced draft legislation on April 8 that would require the government to set mandatory cybersecurity standards for collaboration software. The Oregon Democrat said "vendor lock-in, bundling, and other anticompetitive practices" result in the government spending "vast sums" on insecure software.

Noting the cyber review board's assertion that Microsoft isn't focused on

security, Wyden told Bloomberg: "For a company that is entrusted with as much sensitive government information, particularly one generating tens of billions of dollars in cybersecurity revenue alone, that is unacceptable. Relying on government tech vendors to do the right thing out of the goodness of their own hearts has been a losing strategy for decades."

Microsoft declined to comment on Wyden's draft legislation or remarks. Describing a cybersecurity landscape that has never been more challenging, the company said it has a "unique role to play in keeping the world safe."

'Ground zero'

In an interview at Microsoft's Seattle-area headquarters earlier this month, security chief Charlie Bell described the company as "ground zero" for hackers working on behalf of foreign governments. In part, that's because Microsoft dominates the market for corporate productivity and desktop operating system software.

Recent attacks have struck alarmingly close to home. Early this year, a Russian state-sponsored group was blamed for combing through the email accounts of top Microsoft executives—prompting the company to reassign thousands of engineers to help mitigate the intrusion and accelerate security updates. In May, a hacking gang linked to the Chinese government was accused of stealing one of Microsoft's access tools and used it to break into the email accounts of U.S. Commerce Secretary Gina Raimondo, U.S. Ambassador to China Nicholas Burns and hundreds more, prompting the cyber review board inquiry.

"They're incredibly good at collecting data over time, gathering and gathering more and more momentum and then figuring out how to keep parlaying that into more and more success," Bell said. "It's very difficult

to defend against."

The onslaught, according to Bell, prompted executives to say, "Well, let's step back for a moment."

The result, announced in November, is the Secure Future Initiative, a companywide security reboot that executives say will better position Microsoft to combat current threats as well as future ones that may be turbocharged by artificial intelligence. The effort is being led by Bret Arsenault, a vice president and chief cybersecurity advisor, who served as Microsoft's chief information security officer for 14 years. Asked why the company didn't address the cyber issues sooner, he said the emergence of AI and current hacking trends were among the reasons for a more comprehensive security review.

"There's certain sort of watershed moments or changes in the environment that make you rethink how you want to go do it," he said, later adding that company officials are "energized and focused" on executing the initiative's commitments, "which align to much of what the government is calling for."

Microsoft says it will use AI and automation to make software safer, as well as rely more on programming languages deemed more secure. The company says it's beefing up security protocols to make it harder for hackers to use stolen credentials or access tools to pilfer data. And it vows to respond to security vulnerabilities more rapidly, including mitigating cloud-based problems 50% faster.

It's a daunting task given Microsoft's size and the complexity of its product portfolio. The company offers Windows, Office, Exchange email and other products via the cloud, but continues to provide them to customers with their own servers. In the latter instance, Microsoft offers "patches" for flaws in so-called legacy systems and relies on customers

to install them and maintain security protocols. Customers don't always follow through, and efforts to end support for outdated programs like Windows XP or Windows 7 created an uproar because many were embedded in ATMs, hospital hardware and other critical systems.

"You have a whole bunch of things out there that have to be cleaned up," Bell said. "And that's growing over time."

Microsoft is accelerating efforts to remove old or unused accounts as well as applications that are no longer supported by software updates or meet new security standards. So far, the company has removed more than 1.7 million identities tied to aged or unused accounts and 730,000 apps that were out of date or not meeting security standards, though it wasn't clear how many identities and apps overall might fit that description.

Microsoft is also beefing up its use of multifactor authentication, automatically enforcing it for more than 1 million accounts within the company, including those used for development, testing, demos and production, Arsenault said.

The company now requires a video call between managers and employees or vendors who are creating digital IDs and is issuing short-lived credentials to new workers or vendors—steps designed to make it harder for attackers to impersonate someone or steal their ID. Even users with high-level administrator privileges can no longer turn off multifactor authentication when creating new accounts, Arsenault said.

Michael Daniel, the chief executive officer of the Cyber Threat Alliance, a nonprofit that shares intel about cyber risks and is funded in part by some of Microsoft's rivals, reviewed the company's current efforts at Bloomberg's request. Daniel said they would boost security on the company's platforms, including the cloud, if fully implemented. But

he added that the security revamp doesn't appear to fully address several key issues highlighted by the cyber review board, including an "inadequate" security culture.

'Trustworthy computing'

If Microsoft's current woes sound familiar, it's because the company went through a similar crisis in the early aughts. At the time, computer worms were disrupting computers running Windows. In January 2002, co-founder Bill Gates issued his "trustworthy computing" memo urging software developers to prioritize security.

"So now, when we face a choice between adding features and resolving security issues, we need to choose security," Gates wrote. "Our products should emphasize security right out of the box."

Microsoft halted the development of new Windows features for months to fix the flaws and attempted to create a more security-minded culture among its software engineers

Looking back on that period, Arsenault says it was a simpler time. Because Microsoft was releasing a version of Windows every few years, a pause was possible. That's no longer the case because Microsoft and its rivals update software multiple times a day in the cloud. "It's just a different company," Arsenault said.

In the following years, Microsoft also fell behind Google in search, Apple in mobile devices and Amazon in cloud-based services. The pressure to catch up prompted the company to prioritize speed over security. Microsoft wasn't alone. Many tech companies—keen to cash in on Silicon Valley's explosive growth—embraced an ethos epitomized by the then Facebook slogan: "Move fast and break things."

Microsoft's belated shift to the cloud began about 2010. The move let the company fix security flaws directly, rather than asking customers to install patches. But cloud services presented new security challenges, as the recent breaches have made clear.

Given the sophistication and resources of nation-backed hackers, it may be impossible to completely stop them. Microsoft's security overhaul will help, but critics say the company should again slow down the release of new products to ensure better resilience going forward. Last week, the cyber board urged Microsoft to "deprioritize feature developments across the company's cloud infrastructure and product suite until substantial security improvements have been made."

In fact, Microsoft is racing to capitalize on its early advantage in generative artificial intelligence. Already customers are asking how they'll protect all the new AI programs, Bell said. He's got an answer for them: Buy more Microsoft security software.

Even the cybersecurity unit has caught the AI bug—launching an assistant for security professionals that helps detect and thwart hacking attempts. In the past few weeks, executives have been traversing the U.S. showing off the tool, called Copilot for Security. Early customer feedback for the AI assistant has been overwhelmingly positive, according to Vasu Jakkal, a vice president in Microsoft's security division.

"I have never seen interest like that in any security tool," she said.

https://techxplore.com/news/2024-04-microsoft-hacks-grapples-problem-years.html