LA TRIBUNE
PARTAGEONS L'ÉCONOMIE

Cybersecurity: the White House's roadmap for holding companies accountable to hackers

On the Biden administration's agenda is a desire to better protect critical infrastructure, stronger actions against illegal cryptocurrency exchanges and, most importantly, the prospect of penalties for software vendors who fail to meet their cybersecurity obligations.

Guillaume Renouard

March 15, 2023

The Biden administration intends to pass new regulations aimed at constraining companies providing web infrastructure deemed critical. (Credits: JONATHAN ERNST)

Making software vendors accountable to the law in the event of a breach exploited by hackers is the flagship idea of the new cybersecurity roadmap released by the White House. A strategy that aims to "rebalance the responsibility for protecting cyberspace" by easing the burden that currently falls on individuals, small businesses and local governments.

"The president's strategy fundamentally rethinks the American social contract around cybersecurity," Kemba Walden, the director of national cybersecurity (a position created two years ago), said at a press conference. "We expect more from those who own and operate our critical infrastructure."

Software companies in the firing line

This document is merely a policy direction and does not have the force of law. However, it indicates that the Biden administration intends to pass new regulations aimed at forcing companies providing web infrastructures considered critical (which could include, for example, cloud computing giants) to comply with a certain number of cybersecurity standards. But also to sanction, following a cyber attack, those who do not make their code sufficiently secure.

"Software companies must have the freedom to innovate, but they must also be held legally accountable when they fail in their duty to protect consumers, businesses and critical infrastructure providers," the document reads. "Protecting data and ensuring the reliability of critical systems must be the responsibility of those who own and operate the devices hosting our data."

A false good idea?

This idea divides experts, however. For some, it provides a welcome correction to the laws of the market that drag down security standards. "The market does not encourage software vendors to optimize the security of their products (because they are too expensive, not fast enough to deploy, etc.). So they are naturally led to leave cybersecurity loopholes in them.

"This type of regulation, with the added bonus of a public sector that would require more security measures from private companies contracting with it, would give them a real incentive, which is the only way to get things moving," says Jordan Rae Kelly, who heads the continental U.S. operations of FTI consulting, an international consulting firm, and worked on the previous cybersecurity roadmap produced by the Trump administration.

Joseph Steinberg, a cybersecurity expert and author of the book Cybersecurity for Dummies, meanwhile, worries about the negative impact such a move could have on innovation and competition.

"Such a transfer of responsibility would make it much more difficult for many startups to raise funds, and would discourage entrepreneurs from innovating in certain areas. A startup could go bankrupt because it would be forced to allocate significant resources to a lawsuit filed against it due to a security breach, even if it ultimately won.

Especially since software vulnerabilities do not exist in and of themselves: they often become exploitable once the software is deployed in a specific environment, and as a result of other deficiencies, such as a misconfigured security system or human error."

Other industry professionals question the practicality of such a development. "Conceptually, the idea is good, but a lot of software is open source, with code written not by company employees but by individuals. Does this mean that we're going to blame a cyberattack on Johnny who lives in Slovenia and forgot a bug in his code? That's not realistic. On the other hand, it could put more pressure on new technology companies to provide better cyber insurance policies," says Ralph Echemendia, cyber expert and ethical hacker.

Towards a long legislative road to the cross?

The roadmap also proposes expanding the security measures required in certain sectors deemed critical, where a cyberattack could prove particularly devastating, such as energy, water and health. But also to deploy more resources to fight against illegal cryptocurrency transactions, in order to put obstacles in the way of ransomware attacks, which rely mainly on this mode of settlement more difficult to trace for the authorities. Or invest in cutting-edge cybersecurity research to reap long-term benefits.

Some components of this strategy can be accomplished without legislative changes, according to Jordan Rae Kelly: "For example, the Biden administration could choose to award government contracts only to software companies that meet certain security criteria, or to employ regulators more aggressively."

The Biden administration has used this strategy in the past. For example, after a Russian ransomware attack crippled oil pipeline operator Colonial Pipeline, the White House used the authority of the Transportation Security Administration to force pipeline owners and operators to comply with more stringent security standards set by the federal government. The U.S. Environmental Protection Agency has just done the same with water pipelines.

Since Joe Biden's tenure began, the FBI has also begun using search warrants to find and dismantle malicious code fragments spotted on corporate networks, as well as hacking into ransomware groups to get hold of the codes that allow companies to decrypt malware used against them and thus defuse ransomware demands.

The most ambitious aspects of this new strategy, however, such as holding software vendors liable for cyberattacks, will necessarily require legislative reform, which looks difficult at a time when half of Congress is under Republican control. While cybersecurity may be a bipartisan issue, elected officials in the Grand Old Party are likely to be reluctant to impose more controls on private companies.

Geopolitics as the main obstacle

For Joseph Steinberg, the roadmap also partially misses the mark by leaving out several points that he believes are the major issues that a cybersecurity policy must address today. "First, putting in place the mechanisms that can educate many more Americans about cybersecurity, starting at a young age. Second, preventing hardware and software under the influence of hostile elements, such as China, from operating on American networks. Finally, create a strong, clear, unified framework. Today, there are so many different standards and rules that there is effectively none," he laments.

Since George W. Bush, who started the trend in 2008, it is customary for each U.S. president to define a new cybersecurity strategy during his term. The Trump administration's strategy placed geopolitics at the heart of the cybersecurity issue, highlighting in particular the risk posed by Huawei's dominance of 5G. Compared to the previous strategy, the Biden administration's roadmap places greater emphasis on imposing new rules on private companies, as opposed to the laissez-faire approach favored by Republicans in the domestic market.

On the other hand, it is in line with the Trump administration's findings on geopolitics, which remains the main obstacle facing the U.S. cyber strategy. After the attack on Colonial Pipeline in 2021, Joe Biden tried to get Vladimir Putin to crack down on hackers operating from Russia, but any hope of cooperation in this area collapsed with the invasion of Ukraine. The context of high tensions with China and Russia thus provides a breeding ground for cybercriminals and makes it all the more necessary to adopt a solid cybersecurity strategy.

Guillaume Renouard