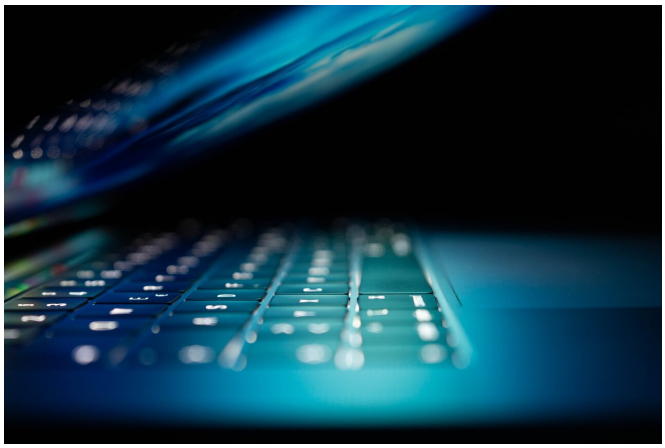
Report: Web security improves, but big gaps remain

22 July 2020, by Peter Grad



Credit: Unsplash/CC0 Public Domain

A report released this week reveals good news and bad news concerning the current global state of security on the Internet. The good news, according to a massive study last spring conducted by the security analytics firm Rapid7, is that despite potential tremors the worldwide outbreak of COVID-19 might have unleashed on the Internet, the system is actually holding up relatively well and security measures are improving.

The bad news is that despite pockets of improvement, there remain gaping holes in security worldwide. The study found websites continuing to use the less secure HTTP protocol rather than newer encrypted options, while organizations continue to utilize outmoded, vulnerable software versions that in some instances were not updated since 2006. One troubling statistic showed more than 3 million databases online continue to allow unencrypted queries and nearly 3 million network routers and switches allow unencrypted notoriously unsecured telnet connections.

Still, Tod Beardsley, director or research for Rapid7, expressed optimism over the results.

"We saw a fairly large drop in [older and less secure] SMB (server message block) and Telnet, our favorite vulnerable punching bags—things that you should never, ever, ever put on the Internet," he said. "So, at least structurally, on a protocol and service basis, the Internet seems to be going in the right direction, which was surprising to us."

In fact, the authors of the report found the lack of chaos in the wake of the epidemic "shocking." "This is a frankly shocking finding," the report states. "The global disasters of disease and recession, along with the uncertainty they bring, appear to have had no obvious effect on the fundamental nature of the internet."

They allowed for the possibility that the full impact of coronavirus has yet to reveal itself.

The 165-page report ranked countries and industries according to the relative security of their internet connections.

Topping the list of "most exposed" countries were the United States, China, South Korea, the United Kingdom and Germany. Rapid7 considered several factors in the rankings, such as "total attack surface," the number of IPv4s exposing vulnerabilities. Given the dominant presence of the United States and China on the web, their prominent spots at the top of the list were not unexpected. The rankings also considered SMB, SQL Server and Telnet exposures and Common Vulnerabilities and Exposures listings.

Rapid7 last year conducted surveys on internet security among leading businesses in major countries. The list of companies was drawn from the Fortune 500 in the United States, the FTSE 250-plus in the United Kingdom, the Deutsche Börse Prime Standard 320 in Germany, the ASX 200 in Australia, and the Nikkei 225 in Japan. Its analysis showed financial services, telecommunications and retail topping the list of

most vulnerable businesses worldwide. At the bottom of the list—those exhibiting the fewest vulnerabilities—were real estate, professional services, hotels and restaurants.

The report also copied an approach New York City uses to evaluate health standards in restaurants, in this instance assigning a letter grade based on the number of web vulnerabilities in each industry category. Only two groups received a top grade of A: Aerospace, defense and transportation (listed as a single group), and motor vehicles. Languishing at the bottom of the list with grades of D were telecommunications, financial services and health care.

The report states that despite improvements globally, none of the industries comes close to being perfect.

Worldwide, "companies have a lot of work to do when it comes to cyber-hygiene," the report states.

The report's authors are optimistic that increasing awareness of potential problems will eventually help make the internet more secure.

According to Bob Rudis, chief data scientist at Rapid7, "Policymakers, business leaders and innovators have an opportunity to shape the security of the internet of the future, but only if they are aware of the state of today's internet."

More information:
www.rapid7.com/research/report/nicer-2020/

APA citation: Report: Web security improves, but big gaps remain (2020, July 22) retrieved 26 June 2022 from https://techxplore.com/news/2020-07-web-big-gaps.html