How Ukraine has defended itself against cyberattacks—lessons for the US

6 April 2022, by Robert Peacock

Credit: CC0 Public Domain

In 2014, as Russia launched a proxy war in Eastern Ukraine and annexed Crimea, and in the years that followed, Russian hackers hammered Ukraine. The cyberattacks went so far as to knock out the power grid in parts of the country in 2015. Russian hackers stepped up their efforts against Ukraine in the run-up to the 2022 invasion, but with notably different results. Those differences hold lessons for U.S. national cyber defense.

I'm a cybersecurity researcher with a background as a political officer in the U.S. Embassy in Kyiv and working as an analyst in countries of the former Soviet Union. Over the last year, I led a USAID-funded program in which Florida International University and Purdue University instructors trained more than 125 Ukrainian university cybersecurity faculty and more than 700 cybersecurity students. Many of the faculty are leading advisors to the government or consult with critical infrastructure organizations on cybersecurity. The program emphasized practical skills in using leading cybersecurity tools to defend simulated enterprise networks against real malware and other cybersecurity threats.

The invasion took place just weeks before the national cybersecurity competition was to be held for students from the program's 14 participating universities. I believe that the training that the faculty and students received in protecting critical infrastructure helped reduce the impact of Russian cyberattacks. The most obvious sign of this resilience is the success Ukraine has had in keeping its internet on despite Russian bombs, sabotage and cyberattacks.

What this means for the U.S.

On March 21, 2022, U.S. President Joe Biden warned the American public that Russia's capability to launch cyberattacks is "fairly consequential and it's coming." As Deputy National Security Adviser Anne Neuberger explained, Biden's warning was a call to prepare U.S. cyber defenses.

The concern in the White House over cyberattacks is shared by cybersecurity practitioners. The Ukrainian experience with Russian cyberattacks provides lessons for how institutions ranging from electric power plants to public schools can contribute to strengthening a nation's cyber defenses.

National cyber defense starts with governments and organizations evaluating risks and increasing their capacity to meet the latest cybersecurity threats. After President Biden's warning, Neuberger recommended that organizations take five steps: adopt multifactor password authentication, keep software patches up-to-date, back up data, run drills and cooperate with government cybersecurity agencies.

Access control

Cyber defense begins with the entryways into a nation's information networks. In Ukraine in recent years, hackers entered poorly protected networks by techniques as simple as guessing passwords or

intercepting their use on unsecure computers.

More sophisticated cyberattacks in Ukraine used social engineering techniques, including phishing emails that tricked network users into revealing IDs and passwords. Clicking an unknown link can also open the door to tracking malware that can learn password information.

Neuberger's recommendation for adopting multifactor password authentication recognizes that users will never be perfect. Even cybersecurity experts have made mistakes in their decisions to provide passwords or personal information on insecure or deceptive sites. The simple step of authenticating a login on an approved device limits the access a hacker can obtain from just gaining personal information.

Software vulnerabilities

The programmers who develop apps and networks are rewarded by improving performance and functionality. The problem is that even the best developers often overlook vulnerabilities as they add new code. For this reason, users should permit software updates because these are how developers patch uncovered weaknesses once identified.

Prior to the invasion of Ukraine, Russian hackers identified a vulnerability in Microsoft's leading data management software. This was similar to a weakness in network software that allowed Russian hackers to unleash the NotPetya malware on Ukrainian networks in 2017. The attack caused an estimated $10 billion in damage worldwide.

Just days before Russian tanks began crossing into Ukraine in February 2022, Russian hackers used a vulnerability in the market-leading data management software SQL to place on Ukrainian servers "wiper" malware that erases stored data. However, over the last five years Ukrainian institutions have significantly strengthened their cybersecurity. Most notably, Ukrainian organizations have shifted away from pirated enterprise software, and they integrated their information systems into the global cybersecurity community of technology firms and data protection agencies.

As a result, the Microsoft Threat Intelligence Center identified the new malware as it began appearing on Ukrainian networks. The early warning allowed Microsoft to distribute a patch around the world to prevent the servers from being erased by this malware.

Backing up data

Ransomware attacks already frequently target public and private organizations in the U.S. The hackers lock out users from an institution's data networks and demand payment to return access to them.

Wiper malware used in the Russian cyberattacks on Ukraine operates in a similar manner to ransomware. However, pseudo ransomware attacks permanently destroy an institution's access to its data.

Backing up critical data is an important step in reducing the impact of wiper or ransomware attacks. Some private organizations have even taken to storing data on two separate cloud-based systems. This reduces the chances that attacks could deprive an organization of the data it needs to continue operating.

Drills and cooperation

The last set of Neuberger's recommendations is to continually conduct cybersecurity drills while maintaining cooperative relationships with federal cyber defense agencies. In the months leading up to Russia's invasion, Ukrainian organizations benefited from working closely with U.S. agencies to bolster the cybersecurity of critical infrastructure. The agencies helped scan Ukrainian networks for malware and supported penetration tests that use hacker tools to look for vulnerabilities that can give hackers access to their systems.

Small and large organizations in the U.S. concerned about cyberattacks should seek a strong relationship with a wide-range of federal agencies responsible for cybersecurity. Recent regulations require firms to disclose information on

cyberattacks to their networks. But organizations should turn to cybersecurity authorities before experiencing a cyberrattack.

U.S. government agencies offer best practices for training staff, including the use of tabletop and simulated attack exercises. As Ukrainians have learned, tomorrow's cyberattacks can only be countered by preparing today.

Provided by The Conversation
APA citation: How Ukraine has defended itself against cyberattacks—lessons for the US (2022, April 6) retrieved 19 August 2022 from https://techxplore.com/news/2022-04-ukraine-defended-cyberattackslessons-theus.html