ECRI Institute

Event Reporting & Analysis - News

Lessons from the Recent Cyberattack that Crippled Computers across the Globe

Published 5/26/2017

Britain's National Health Service (NHS) was the highest-profile victim of a worldwide ransomware attack that crippled computers in nearly 100 countries on May 12, 2017. More than 90% of NHS computers were using Windows XP, a 15-year-old operating system that made them susceptible to the attack, according to a May 13, 2017, article in *The Guardian*. Microsoft released a software patch to fix the problem in March, but a large number of organizations did not install it. NHS issued a warning Friday morning that "a serious ransomware threat" was imminent, but it proved impossible to stop. Patient records, phone lines, and e-mails were rendered inaccessible at health facilities across Britain, forcing staff to use pen and paper, as well as their personal mobile phones. The ransomware displayed a pop-up message that said computers would be inaccessible unless a ransom of $300 per infected computer was paid in online currency. One worker quoted in the story said the attack appeared to be the result of someone opening an e-mail attachment. As of May 15, some British doctors still did not have access to full patient records, according to an article in the *New York Times*, and some patients may have postponed medical care. New cases appeared in Asia over the weekend and experts believe the threat is not over, according to another article in *The New York Times*. The U.S. government said the most up-to-date information about the attack is available at the United States Computer Emergency Readiness Team's (US-CERT) website. US-CERT advised people to only open emails from people they know. Users should click on attachments and links only if they were expecting to receive one, since attackers can impersonate a sender. Organizations should also keep their antivirus software up to date as another layer of security. They are also advised to find out which version of Windows they are running. Part of the reason the attack was able to spread so quickly is that the attackers targeted large institutions, which are known to have out-of-date security systems, according to a May 13, 2017, article about the security response in the *New York Times*. Microsoft's president and chief legal officer wrote that the attack is a "wake up call" that cybersecurity is a shared responsibility between the technology industry, governments, and computer users.

TOPICS AND METADATA

Topics

Health Information Privacy; Security/Safety

Caresetting

Ambulatory Care Center; Ambulatory Surgery Center; Emergency Department; Hospital Inpatient; Hospital Outpatient; Physician Practice; Short-stay Facility; Skilled-nursing Facility

Roles

Healthcare Executive; Regulator/Policy Maker; Risk Manager; Security Personnel

Information Type

News

Publication History

Published May 26, 2017