Monthly Cybersecurity Newsletter

March 2020 Issue

NC DIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

Top 7 Cybersecurity Trends for 2020

TÜV Rheinland's seventh annual report on Cybersecurity Trends for 2020 (a collaboration between many cybersecurity experts globally), identified seven key cybersecurity trends we should be aware of in 2020.

Peter Láhner, business executive vice president for the business stream Industry Service & Cybersecurity at TÜV Rheinland, stated: "From our point of view, it is particularly serious that cybercrime is increasingly affecting our personal security and the stability of society as a whole … One of the reasons for this is that digital systems are finding their way into more and more areas of our daily lives. Digitalization offers many advantages – but it is important that these systems and thus the people are safe from attacks."

Here are the top seven cybersecurity trends that TÜV Rheinland cybersecurity researchers and experts say you should be aware of in 2020:

1. Uncontrolled access to personal data carries the risk of destabilizing the digital society. In 2017, a French woman, Judith Duportail, asked a dating app company to send her any personal information it had about her. She received an 800-page document containing her Facebook likes and dislikes, the age of the men she'd expressed interest in and every single online conversation she'd had with 870 matching contacts since 2013. The fact that she received so much personal data after several years of using a single app underscores the fact that data protection is now very challenging.

2. Smart consumer devices are spreading faster than they can be secured. The number and performance of individual "smart" devices – such as smart speakers, fitness trackers, smart watches, thermostats and smart home security cameras – is increasing every year, making them a very attractive target for cybercriminals. With the proliferation of smart devices, the attack surface could quickly increase hundreds or thousands of times.

3. The trend toward owning a medical device increases the risk of an internet health crisis. Over the past 10 years, personal medical devices, such as insulin pumps, defibrillators, pacemakers and heart and glucose monitors have been connected to the internet as part of the "Internet of Medical Things" (IoMT). Researchers have identified a growing number of software vulnerabilities and demonstrated the feasibility of attacks on these products, which can lead to targeted attacks on both individuals and entire product classes.

4. Vehicles and transport infrastructure are new targets for cyberattacks. Through the development of software and hardware platforms, vehicles and transport infrastructure are increasingly connected. The

disadvantage is the increasing number of vulnerabilities that attackers could exploit – broad cyberattacks targeting transport could affect not only the safety of individual road users but could also lead to widespread disruption of traffic and urban safety.

5. Hackers target smart supply chains and make them "dumb." With the goal of greater efficiency and lower costs, smart supply chains leverage Internet of Things (IoT) automation, robotics and big data management – smart supply chains increasingly represent virtual warehousing or any place where a product or its components can be located at any time. Nevertheless, smart supply chains are dynamic and efficient but are also prone to cyberattacks.

6. Threats to shipping are no longer just a theoretical threat but a reality. Many aspects of shipping can be vulnerable to attack, such as navigation, port logistics and ship computer networks. There's ample evidence that hostile nation states and activist groups are experimenting with direct attacks on ship navigation systems and attacks on the computer networks of ships to extort ransom.

7. Vulnerabilities in real-time operating systems could herald the end of the patch age. In 2019, Armis Labs discovered 11 serious vulnerabilities (called "Urgent/11") in the real-time operating system (RTOS) Wind River VxWorks. Six of these flaws exposed an estimated 200 million IoT devices to the risk of remote code execution (RCE) attacks. This level of weakness is a major challenge as it's often deeply hidden in large numbers of products, and organizations might not notice that these vulnerabilities exist. In view of this, the prediction the practice of installing the latest security updates will become ineffective.

REMINDER: Stay Safe During Tax Season

Here are a few resources that can help you protect your identity and be safer and more secure online this tax season – and year-round:

- Staying Safe from Cybercrime During Tax Time
- STOP. THINK. CONNECT.™ Tips and Advice
- Identity Theft Resource Center
- The Federal Trade Commission's IdentityTheft.gov
- The IRS's Tax Scams and Consumer Alerts

Increase in Ransomware Attacks Predicted in 2020

By Scott Couch | FOX 17 Nashville | Sunday, January 12th, 2020

NASHVILLE, Tenn. -- In the past two years, hackers have taken over the computer systems of cities across the country including Atlanta. They demand a ransom to regain control, (usually paid in untraceable Bitcoin). In the past 90-days, ransomware victims include: New Orleans, Louisiana, Pensacola, Florida and Johnson City in East Tennessee. Jeff Schwartz, VP of Check Point Software Technologies, a global provider of "IT" security software and among the vendors metro government pays to help keep hackers away, predicts an increase in ransomware attacks in 2020. Watch the complete 2:38 video news report for the full story.

CORONAVIRUS: Security Awareness Tip of the Month

Federal health officials expect the coronavirus to spread to the U.S., and that's good news for hackers.

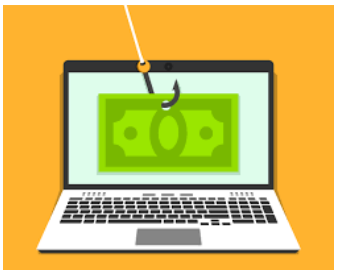
Cyberthreat actors leverage interest during public health threats and other high-profile events to conduct financial fraud and deliver malware by posting links to fake charities and fraudulent websites that solicit donations for relief efforts.

The Center for Internet Security's Multi-State Information Sharing and Analysis Center observed similar scams and malware dissemination campaigns in response to previous high-profile events including Hurricane Harvey, the Boston Marathon bombing, the Royal Wedding and the Tennessee wildfires.

Its highly likely that more scams and malware will follow over the course of the response period. Internet users should exercise caution before opening related emails, clicking links, visiting websites or making donations to coronavirus relief efforts.

For the full article, visit https://www.cisecurity.org/newsletter/cyber-threat-actors-expected-to-leverage-coronavirus-outbreak/.

March Madness & Phishing Scams



March Madness is just around the corner, and cybercriminals are ready to take advantage of the hype surrounding your favorite college teams and their basketball championship quests through phishing schemes.

It's a perfect opportunity for them to use phishing schemes to steal personal information from unsuspecting fans filling out online brackets, buying tickets and merchandise or streaming live video.

Phishing is a form of social engineering that uses email or malicious websites to get personal information by posing as a trustworthy source to gain access to your accounts.

Here's some signs things to be on the lookout for:

- **Suspicious sender's address.** The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.

- **Generic greetings and signature.** Both a generic greeting—such as "Dear Valued Customer" or "Sir/Ma'am"—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.

- **Spoofed hyperlinks.** If you hover your cursor over any links in the body of an email, and the links do not match the text that appears when hovering over them, the link might be spoofed. Additionally, cybercriminals might use a URL shortening service like Bitly or TinyURL, to hide the true destination of the link.

- **Malicious websites.** They might look identical to legitimate sites, but check the spelling of the organization's name and the URL very closely for discrepancies, such as the spelling of the name or the domain (e.g., .net instead of .com). When in doubt, avoid the website until you're 100% sure.

- **Insecure websites.** Check to make sure the websites you're visiting use SSL protection. The easiest way to tell is to check your browser's address bar. Look for https in the URL. Sites without the "s" are not safe to submit payment information or other personal details.

- **Offers too good to be true.** Free games and merchandise or unbelievable deals might be tempting, but they can come at a cost to your privacy. Only download from trusted sources, even if you must pay.

- **Spelling and layout.** Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.

- **Suspicious attachments.** An unsolicited email (especially if it appears urgent or wants you to do something) requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal might use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

CYBERSECURITY NEWSLETTERS

Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4.
***Note**: You must have a valid State employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). This month's edition is titled ***Cyber Threat Actors Expected to Leverage Coronavirus Outbreak***.

- https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Social Media Privacy.***

- https://www.sans.org/security-awareness-training/ouch-newsletter

March 12: Webinar – Protecting Our Communities: Signs of Terrorism, What to Look For, and How to Help Law Enforcement

March 17: Webcast – Women in Cybersecurity: A SANS Survey

March 19: Webcast – Anatomy of a Cloud Data Breach

March 24: Webcast – Women in Cybersecurity: A SANS Survey Panel Discussion

---

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. You are also encouraged to review Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember…Stop. Think. Connect.*