10 Cybersecurity predictions for 2020

With data breaches hitting headlines daily, security professionals are constantly concerned about the next big threat. Whether it's ransomware, phishing or endpoint attacks, there's always something on the horizon waiting for its turn in the spotlight.

Source: pixabay.com

KnowBe4 has compiled a list of its top 10 cybersecurity predictions for 2020 from its executive leadership team and an array of security awareness advocates from around the world. The topics range from upcoming government legislation to security culture to specific industry verticals being targeted in cyber attacks.

1. In 2020, federal legislation will be passed that makes any ransomware infection of more than 500 records automatically a data breach with all the resultant disclosure requirements and legal expenses.

2. We will see further Balkanisation of the internet and its services. While countries like China have traditionally maintained its own infrastructure, we have seen political issues spill out to the cyber realm, with companies like Kaspersky and Huawei being banned in the U.S. We will likely see more products and services having to be tailored for local requirements and regulations.

3. A nation-state will decide to make a point and flex their cyber muscles by initiating large-scale manipulation of everyday consumer IoT products. In addition to the general panic and unease that is caused, other – even more series – impacts will reign across power grids and aspects of critical infrastructure.

4. Social engineering and unpatched software will remain the top two root causes for successful exploits as they have been for over three decades. Everyone knows they are the top two causes, but most of the world will not treat them like the top threats they are. Instead, they will be mostly ignored or weakly mitigated while most of the world concentrate more resources on things less likely to happen.

5. We'll see more targeted multi-vector attacks emerge. The bad guys are building increasingly more complex attacks to combat the increasing layers of defence. And while defensive measures are in no way sufficient in battling various attacks yet, the bad guys are always looking to increase the efficiency of their attack methods. Combining a multi-attack vector to chain-link attacks is an excellent way to increase efficiency and reduce the cost of an attack, which allows them to scale up even more.

6. Business email compromise will escalate and cause major disruption to day-to-day activities across the globe, leading to the addition of compulsory new-school security awareness training and testing in business, academia, industry and government. This will, in turn, result in collaboration and sharing of 'near misses' related to cyber threats more than ever. At present, there is a lot of caution with sharing such information.

7. Deepfake technologies will be used to attempt to influence the 2020 elections in the United States and beyond. Fake videos and audio will be released close to the election time in order to discredit candidates or to swing votes. While these will be proven as fakes fairly rapidly, undecided voters will be influenced by the most realistic or believable fakes.

8. In 2020, the use of the term security culture will continue to increase as more organisations understand what it takes to reduce risk and manage security in their workforce. A combination of training, assessments and a structured process is being implemented to manage the human factors that influence security.

9. As energy facilities continue to be targeted for cyber attacks, the need for Operation Technology (OT) departments and Information Technology (IT) to collaboratively solve the cybersecurity issues will be increased importance for organisations. They will need to collaborate with their own corporate Security Operations Center (SOC) or utilize virtual SOCs to continually monitor their SCADA or DCS networks monitoring network activity and assets connecting and disconnecting from the networks.

10. Governments such as China, Russia – and as seen more recently with Saudi Arabia's recruitment of a Twitter employee – will continue to pose counterintelligence (i.e., insider) threats to corporate America and our allies. The media is replete with stories regarding insider threats posed by our acknowledged adversaries and some "uneasy" allies. There is no return on investment to spend millions of dollars in time, money and effort to cyber access to a network when an intelligence service can spend less than $100,000.00 to gain the information they need by recruiting a willing employee with financial (or otherwise) vulnerabilities.

    Any organisation with significant personally-identifying information, especially as it relates to people in countries with politically vulnerable populations, should pay special attention to their insider threat education efforts.

Conclusion

There's no doubt that it will be interesting to see what the future holds for the cybersecurity industry in 2020. Most importantly, users should remember to think before they click.

Security professionals should remain vigilant and keep these upcoming threats and trends in mind when thinking about the overall security of their organisations in 2020 and beyond.