WHY 2019 CAN GIVE CYBER DEFENDERS 20/20 VISION

Organizations are struggling to defend against cyberattacks, with the average cost of a data breach totaling to $3.92 million.¹ Last year, consumers lost $1.48 billion to identity fraud.² This National Cyber Security Awareness Month, we take a look back at the top cyber incidents and trends spotted so far this year and examine what it all means for the future.

LOOKING BACK AT 2019

GEOPOLITICAL TENSIONS
Nearly 75% of CEOs say their companies are affected by geopolitical cyber attacks, but only 15% feel resilient.⁷

In July, Microsoft revealed 8,000 of its enterprise customers have been targeted by nation-state hackers over the past year, indicating that bad actors are continuing to use cyber as a tool offensively.⁸

Space has become increasingly appealing for foreign adversaries. The U.S. has more than 1,800 space satellites, providing critical services such as GPS, cell phone and Wi-Fi connectivity, which expands the attack surface to infiltrate our systems.⁹

NO INDUSTRY IS SAFE
More than 70 state and local governments were infected with ransomware this year.¹⁰

The aviation industry is a top target, averaging 1,000 attacks per month.¹¹ Today, 90% of aircraft run on legacy systems designed in the 70s and not built with security in mind.¹²

Financial services are also at risk, with the Capital One breach on July 19 compromising the identities of nearly 106 million customers and applicants.¹³

PROTECT 2020
34% of local jurisdictions were using voting machines over 10 years old as their polling equipment during the 2018 midterms, including counties and towns in 41 states.¹⁴

In 2016, 27.5 million voters cast their ballots on paperless machines. As many as 16 million will do so in 2020.¹⁵

A federal government spending bill granted $380 million to help safeguard U.S. voting systems from cyber attacks. A significant portion of these funds will be used to Protect 2020.¹⁶

RANSOMWARE
Ransomware incidents increased by 118% during the first quarter of 2019 with ransomware causing 10 days of downtime, the equivalent of $72 million lost.¹⁷

Of the cities attacked in 2019, Baltimore and Atlanta have been in the spotlight. Each has spent an estimated $17-18 million on recovery.¹⁸

SECURING TOMORROW

OWN IT: YES, IT’S YOUR RESPONSIBILITY
Organizations, their employees and their contractors need to take greater responsibility when it comes to cybersecurity culture. We’ll continue to see devastating breaches like Capital One happen if we don’t emphasize a security-first culture, where each person recognizes how their actions play a role in the greater security of an organization.

SECURE IT: SECURITY FROM INCEPTION

Organizations will continue to invest in new applications and infrastructure, and security must be baked into everything from DevOps to cloud adoption. Reference architectures like zero trust can provide the right frameworks to do these things securely from the outset, rather than relying on the SOC or point security products to secure systems after the fact.

PROTECT IT: THE BIGGER PICTURE, OUR DEMOCRACY

Through attacks on our election critical infrastructure, adversaries attempt to undermine our nation’s democracy by seeding doubts of legitimacy. To combat this, we need to strengthen our global collaboration and develop a cyber doctrine that allows us to better protect our democracy and rebuild the nation’s trust in these processes.

¹. IBM Security, How much would a data breach cost your business? 2019
². IdentityTheftResourceCenter, Fact: Identity Theft Frequency 2016
³. Health IT Security, Ransomware Attacks Close in on 2016, Drive-Byte Attempts Increase 2018
⁵. Gartner, The Cost of Downtime, 2014
⁶. Raytheon, Threat Spotlight - Government/Ransomware Attacks, 2019
⁸. Reuters, U.S. speeding up to provide $380 million for election cyber security 2019
⁹. TechRepublic, State and local governments increasingly targeted by ransomware attacks 2019
¹⁰. EYACTIC, hacker-bombard aviation sector with over 1,000 attacks per month 2016
¹¹. National Training Aircraft Symposium, Aviation Cybersecurity: An Overview 2018
¹². CNN, Capital One data breach: What you can do now following bank hack 2019
¹³. TechRepublic, 2 ways geopolitical attacks could impact your business this year 2019
¹⁴. Microsoft, New cyberthreats require new ways to protect democracy 2019
¹⁵. United Nations Office for Outer Space Affairs, Outer Space Objects index