2018: WHAT MATTERED IN IT?

downs.

Jeffrey Burt | Dec 26, 2018

Cybersecurity continues to be a key concern in an IT industry that often seems under siege by new and increasingly sophisticated attacks launched by ever-morphing combinations of threat actors, cybercrime groups and nation-states.

The ransomware scourge of 2017--while certainly still a significant threat--found itself replaced at the top of the charts this year by malware that steals CPU cycles from victims' computers to illegally mine cryptocurrencies like Bitcoin and Monero. The punch-counterpunch battle between security firms and cybercriminals continued unabated and promises to accelerate as the use of artificial intelligence and machine learning capabilities grows on both sides, and evidenced in recent security breaches.

But while cybersecurity primarily is seen as a software issue, the industry entered 2018 facing vulnerabilities at the hardware level that have been around for decades. Given the nature and long-ranging impacts of the Spectre and Meltdown vulnerabilities, that's probably the best place to start when looking at some of the top security stories from 2018, before delving into recent security breaches, like Marriott.

Spectre and Meltdown

The news: Google's Project Zero team found the vulnerabilities in processors in 2017 but worked with chip makers and software vendors before making their revelations public in January 2018.

Why it mattered: The announcement of Spectre and Meltdown shook the industry because the vulnerabilities were in chips that have been in use for a couple of decades. Initially seen as an Intel problem, it quickly became apparent that the technique linked to the vulnerabilities--speculative execution, used to increase the performance of processors--also impacted AMD's x86 chips as well as those using the IBM Power, SPARC and ARM architectures. Things were further complicated in the months following because of the discovery of multiple variants of both Spectre and Meltdown.

problem for somewhere between 15 and 20 years, so there are lots of processors out there that have these holes in various forms. We've also got to build better mechanisms" to ensure security in hardware.

How this affects IT: Professionals will need to ensure that hardware checks are now part of their routine security scans.

Breaches

The news: It's impossible to look at an entire year in cybersecurity without highlighting the significant data breaches that occurred, and in that sense, 2018 was little different than other years.

Why it mattered: Despite ever-new solutions for protecting businesses' cyber-environments and the breaches of previous years serving as warnings to organizations to protect their data, a large number of companies were hit by hackers this year in the form of recent security breaches that impacted tens of millions of users.

How this affects IT: No vertical is secure -- so no IT pro is immune to a breach. A hack of Marriott International in November exposed the personal data of more than half a billion guests. Other recent security breaches: Under Armour in March revealed that the information of about 150 million users of its MyFitnessPal nutrition app was compromised, the personal and financial details of about 380,000 British Airways flyers were exposed in a hack in August and September. Most recently, question-and-answer site Quora said account data of about 100 million users was compromised after a third-party hacker accessed the company's computers. This hit list continues, with Ticketmaster (40,000 users had personal data compromised), MyHeritage (92 million), T-Mobile (2 million), HSBC

The news: Attention to the issue of privacy grew in 2018 among consumers, vendors and lawmakers. Unsurprisingly, Facebook was at the center of much of the debate. The social networking giant, which has often given privacy little more than a passing nod, earlier in the year found itself at the intersection of privacy and politics when a report revealed that data from 87 million of its users had been grabbed by Cambridge Analytica without their consent and used for political reasons during elections in 2016. Though the first reports emerged in 2015, it wasn't until this year that the scandal blew up following the emergence of an ex-Cambridge Analytica employee as a whistleblower. Facebook now finds itself in the middle of another privacy debate after documents released by British Parliament showed that company officials had put a specific monetary value on user data, even though they have said Facebook uses such data only to sell ads. It was more fuel for the argument that with Facebook, users are not the customers, but the product.

Why it mattered: But privacy in 2018 wasn't only about Facebook. The European Union's long-anticipated General Data Protection Regulation (GDPR) finally went into effect in May, with strict rules about the handling of user data for any company with EU residents as customers and potential steep penalties for organizations found violating those rules. California in June enacted its own data

Apple, Google, Microsoft, Facebook and other tech companies that make up the group Reform Government Surveillance (RGS) pushed back against efforts by the Department of Justice and FBI to convince tech companies to add backdoors to products and services. The RGS argued that proposals by law enforcement officials would weaken the encryption that protects devices and make them more insecure, opening them up to attacks.

How this affects IT: Compliance is going to be an ongoing concern for security professionals.

IoT and Security

The news: The Mirai virus that emerged in 2016 launched massive DDoS by taking control of such devices like printers and baby monitors. Security pros have shown how everyday systems like a connected television can be hacked, and once bad actors get into the system, they can move into the network. And researchers at Trend Micro issued a report about weaknesses in MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol), both key protocols for the IoT and industrial IoT (IIoT).

Why it matters: With some estimates of connected devices reaching 25 billion by 2020, the Internet of Things (IoT) is getting a lot of attention from cybercriminals, cybersecurity vendors and lawmakers alike. The rapid growth in the numbers of intelligent, connected devices--from the smallest sensors and children's toys to medical products, home security cameras and systems on factory floors--is greatly expanding the attack surface for both businesses and consumers, and hackers are taking advantage. Lawmakers are finally taking note of the risks posed by all these connected devices. The House of Representatives in late November passed the

How this affects IT: California officials this fall enacted the country's first IoT security legislation that requires the makers of the connected devices to equip their products with security features to protect both the operation of the device as well as the data it collects and stores. However, there are exceptions, including ensuring that manufacturers aren't responsible for third-party applications that users add to the devices and doesn't apply to devices bought for resale.

TAGS: CLOUD SECURITY