ANOMALIX

ANOMALIX
WHITE PAPER
Cybersecurity Trend for 2019

Cybersecurity Trends for 2019

This past year saw an explosive growth of applications, sensors, and technologies designed to improve information flow between companies, customers and business partners. While these technologies increased the flow of information, they also heightened the potential for cyber-attacks both inside and outside of the organization.

As companies integrate IoT, Cloud Computing, Artificial Intelligence, and Machine Learning technologies, the likelihood of attacks will increase. The implications are far-reaching, and include not only degradation of data, but a higher potential for business interruption. It is no longer a question of if an attack will happen, but if your organization is prepared when an does attack occurs.

As companies become dependent on real-time and intense volumes of data, it is imperative that they not only continue historical methods of preventing breaches but also implement a proactive approach to anticipate attacks. Attackers with malicious intent desire access to your network and will go to great lengths to accomplish their goal. .

IOT

Gartner research projects over 20 billion IoT units to be installed by 2020, or approximately four units per each human on earth. IoT sensors are in common use, for biometrics, healthcare, supply chain, manufacturing, and virtually every industry. With this growth comes cybersecurity gaps that have far reaching effects.

Security is the number one barrier to IoT growth, according to Gartner. The growth of sensors creates countless endpoints, presenting a massive landscape for firms to monitor. The transfer of real-time data adds additional complexity to this growing technology.

IoT sensors open the doorway for hackers to access corporate networks. While the data captured by the sensor can be valuable, this access vulnerability is a goldmine for hackers, who can now penetrate corporate databases at a cheap price using readily available, open sourced tools.

Consumer Use

The Under Armour's MyFitnessPal tracker hack of 2018, affecting 150 million people, revealed opportunities to collect personal data and commonly used trackers. This vulnerability underscored an inherent weakness in a relatively young industry with explosive growth.

Supply Chain

The highest growth area for IoT cyberattacks is within supply chains. Sensors used in transportation, warehousing, and manufacturing open a doorway for hackers to access vulnerable networks. Once accessed, third parties have access to critical financial, manufacturing, corporate intelligence, and customer data that cancollapse a firm or ruin a market reputation overnight.

Password Vulnerabilities

A study by security firm Symantec revealed that IoT hacks are often accomplished through use of simple passwords and usernames. The most frequently used usernames were “root”, which accounted for up to 50% of hacks in November 2018, followed by “admin” which accounted for over 25%. Passwords “123456” and “[BLANK]” accounted for nearly 60% of incidents. Serial numbers of devices from Wi-Fi routers and connected devices are also a vulnerable piece of data captured and used in concert with passwords.

Homes and Commercial Buildings

The growth of smart systems used to control heating and ventilation systems, security systems, electrical and home appliances creates a vulnerability in consumer and commercial market networks. Once accessed via a vulnerable network, a malicious party can control temperature, utilities, and first responder notification devices, leaving patients, consumers, employees, and other vulnerable parties at the mercy of the attacker.

Corporations can address these problems by identifying all sensors and operation and placing them behind a firewall. Protecting passwords and serial numbers will also address vulnerabilities. Finally, the industry is dependent on professionals who continue to grow and expand their knowledge in this area.

Cloud Computing

Cloud computing has attained widespread adoption as firms moved to Infrastructure as a Service (IaaS), and Software as a Service (SaaS). The growth of these technologies has allowed businesses to lower expenses as they turn to vendors to provide needed software. But convenience comes at a cost as customers may unwittingly download malware, ransomware, bots and viruses from their service provider.

Crypto Mining

Crypto Mining attacks grew by 8500% in 2017, according to Symantec. A relatively new industry, crypto miners don’t necessarily launch malicious attacks but hijack your computer processors and cloud resources to perform mining. As the value of cryptocurrencies increase, so do the mining attacks, draining resources you need to run business operations.

APIs

APIs offer a gateway into computer networks if not secured. T-Mobile experienced a brief attack through a vulnerable API that affected a small percentage – only 2 million – of their 76 million users. APIs integrate business partner and customer networks, allowing data to more easily flow. Many APIs are readily available on the web, and attraction for attackers, and will grow in use

Cloud-based storage

While many firms use cloud-based storage, they may not know what is actually stored in that cloud. A study by Digital Shadows revealed a treasure trove of data – over 1.5 billion files of sensitive data – stored in an open cloud easily accessible via the Internet. Cloud providers are shifting risk to their customers, increasing the importance of access management to stored data. Act-On predicts that by the year 2022, 95% of cloud security issues will be the customer's fault.

Gartner recommends a thorough requirements analysis, architectural planning, and expertise development to offset future attacks.

Artificial Intelligence

Artificial intelligence solutions are expected to grow 36%annually through 2023. As organizations continue to transform their digital presence using AI, advanced security risks come to light.

Explosive data growth

Now that firms have readily adopted AI, the need for mass volumes of data is increasing. Marketing, Product Development, and Business Intelligence departments gather data in an effort to predict consumer behavior and provide new, personalized product offerings. This growth comes at a price, as extensive data sets are a magnet for attackers. Unless security protocols are in place, a company's proprietary data – and their business reputation –can disappear overnight.

SMB growth and Vulnerability

PS Market Research reports that midsize firms are in greatest need of AI solutions to protect and sustain their growth. From customer service chatbots to market analytics, small and midsize firms will take advantage of AI–based offerings, including enhanced security approaches. Attackers are now targeting vulnerabilities in small and medium-sized business infrastructures to collect customer, payment, and sensitive organizational data.

AI used by hackers and defenders alike

AI Solutions offer unique advantages to businesses and individuals. For business, AI means enhanced productivity and customer solutions that lead to greater profits. Individuals benefit from personal health data and connection to remote providers. But attackers are now using AI to access business and personal databases where they can leverage, ransom, or sell the information.

Machine Learning

Machine Learning (ML), combined with AI, creates a powerful combination for companies to learn and predict behavior patterns. Both technologies have made rapid advancements in recent years with new business solutions being brought to market. These technologies are not without security threats and are ultimately dependent upon the people who have access to the large volumes of data they require.

"Learning" to do it right

Programs require massive amounts of data to be interpreted for patterns. ML opens the doorway to discover behavior patterns based on statistical data that was previously inaccessible. While algorithms continue to evolve, the security protocols in place to protect them remain deficient. ML programs can be taught to review system logs and identify outlying behaviors that may indicate a security threat. These ML–generated security protocols use predictive analysis to identify threat levels. As long as the data they are fed is authentic, these protocols are a security enhancement. Unfortunately, attackers are also using the same ML – generated algorithms to create advanced hacking models.

Symantec's global information network (GIN) collects telemetry from 175 million endpoints that include 80 million web proxy user sand 63 million email users who generate over 8 billion reputation requests per day and over 20 trillion security events per year. Analyzing this much data and developing appropriate security responses would be virtually impossible without ML technology.

Adversarial Machine Learning

ML is dependent upon the type of data from which it learns. If a hacker knows what type of data is "feeding" the algorithms, it can attack through a poisoning (contamination of new incoming data) or an evasion (misclassification of current data) tactic. Different levels of access to data may also be exploited, depending upon existing vulnerabilities in your system. In any event, ML data must be secure to avoid unintended, malicious outcomes.

ML programs require continual training. Through repeated review of algorithms and output, security professionals and attackers alike will continually train the systems to meet their intentions – whatever they maybe. That could be why according to a Carbon Black report, 70% of security professionals believe attackers can bypass machine – learning driven security protocols.

Where to begin?

Understanding where your organization is connected to customers, vendors, and third parties is the first step to understanding the security landscape. These connections serve as external pathways into your most valuable asset: your network. Identify vulnerabilities in internal security protocols, including encrypted passwords and access points. Finally, prioritize your identified gaps, addressing the highest risk items first.

Conclusion

Anomalix can solve your IoT and Industry 4.0 challenges by building custom solutions to properly define governance processes, policies, and lifecycle management. As trusted advisors, our Subject Matter Experts (SME) begin by defining business initiatives and determining how IoT devices can be integrated into the security infrastructure before creating a roadmap to adopt new devices.

What are the results?

- **Identify All Connected IoT Devices.** By identifying all devices connected to you network, security programs gain visibility into all potential access points. Once devices are identified, define access governance processes, policies, and lifecycle management. This allows your organization to secure itself while also creating a program for new devices to be added in the future.

- **Cloud computing.** Inventory all cloud resources, including vendor files, and intended purposes. Identifying where files are located and implementing access management rules will reduce existing vulnerabilities.

- **Artificial intelligence.** Identify what AI programs and devices you currently use and their integration with your network. Once data sources are secured, implementing AI programs will produce more effective results.

- **Machine learning.** Effective machine learning algorithms are dependent upon accurate and consistent data. Periodic review of machine learning inputs and outputs will help identify if any outside parties have manipulated your data.

Finally, the basics are essential. Simple, unencrypted passwords are still the primary vulnerability that attackers exploit. Examining and upgrading password systems creates an immediate security enhancement, protecting valuable data and limiting access. Addressing access management approaches, risk management, and monitoring potential threats are still the foundation of security programs for the future.

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144