Inside this Issue Vol 3: Issue 4/19

Cyber Tips

How to stay safe on line.

Cybercriminals have become quite savvy in their attempts to lure people in and get you to click on a link or open an attachment.Read more >>

The Biggest Cybersecurity Targets

Organization have a number of digital assets that cybercriminals want. Mainly, they want money, but usually, they'll take anything they can get, and that can be confidential information. >>

Institute Of Forensics & ICT Security | November 2019 www.forensicsinstitute.org

Forensics & Cyber Security Newsletter

Your source of forensics, security and fraud insights

The Biggest Cybersecurity Targets: Senior Executives

Organizations have a number of digital assets that cybercriminals want. Mainly, they want money, but usually, they'll take anything they can get, and that can be confidential information. Organized crime is targeting everyone on the internet, and malicious hackers are major players who will drive expected global cyber damages of $6 trillion per year by 2021.

These malicious hackers can also encrypt your data, right on your computers and then hold the decryption key for ransom while behind the scenes your data is being copied by the criminals for future exploitation. If trade with customers from your website, it could be shut down by a massive denial of service attack that costs pennies to launch against you for long periods of time.

Senior Executives as targets

Senior executives are among the favorite targets of malicious hackers. WHY? In part because they are more likely to hold valuable information — or have

Short Courses for November

Writing a fraud investigation report
11th &12th | 6pm-8pm | $50

VPN Configuration & Management
18th & 19th | 6pm-8pm | $50

Cyber Security for Cloud Computing Training
20th & 21st | 6pm-8pm | $50

Cyber Security for Cloud Computing Training
20th & 21st | 6pm-8pm | $50

Contract and procurement fraud
25th &26th | 6pm-8pm | $50

a high level of access to such data but mainly because they usually don't take time to concern themselves with the technical bits of cybersecurity and low-level business operations. It is therefore imperative for organizations to make sure that the top management officials are cyber vigilant and are adhering to the most stringent data protection and cybersecurity policies.

Top executives make succulent targets, especially when travelling abroad for business ventures. In such scenarios they often connect to open wi-fi networks in restaurants and airports, use their credit cards for purchases, and encounter moments of fatigue during flights in which they will sleep off and leave their gadgets completely exposed.

The kind of attacks executives face

Email attacks. If you think about it, top executives receive the most important emails about the business that they are running. Usually these emails are downloaded onto the mobile devices, and if such information falls into the wrong hands, it could be catastrophic for the business. Most executives are still unaware that email communication is one of the least secure ways to communicate online.

Phishing attacks and ransomware are the more common ways to get executives to provide the vital information needed to steal data. In this, hackers will use fake website and redirect URL's to dupe executives into giving up their login credentials. To make matters worse in this regard, executives usually want to be connected to up to date company information while using a singular device thereby creating a single point of attack.

Open wi-fi networks. We all enjoy using free things, and there's no free thing that is more exciting than free wi-fi. These open wi-fi hotspots are located in almost all public places. To a senior executive moving in a country where he will not spend long enough to necessitate acquisition of a local ISP, free internet is a real temptation. What these executives do not know is that as you connect to an open wi-fi hotspot, your data will be unencrypted and your device can easily be hacked and a reverse payload injected. These reverse payloads will connect back to the attacker no matter where you go on the planet. It is advisable to use VPN's while connecting to such networks.

Device cloning. As business executives travel through airports and cross borders, a malicious attacker that is good at social engineering can easily clone a device or copy its data in a matter of seconds. It is therefore imperative that such executives do not travel with company sensitive devices with confidential information.

What can be done to secure the senior executives?

Effective security, now more than ever, requires an understanding of how information is accessed and used at all stages, at all times of day and in all variety of locations. Steps have to be taken to protect these executives as they conduct business world wide.

The best way to protect these executives is through training them about the dangers that are lurking and waiting to pounce.

It is with this in mind that IFIS has designed a new course; Cybersecurity for Senior Executives -

https://bit.ly/2NVjR2x

This course will be your Moses that will guide you through the desert of cyber knowledge deficiency, to the promised land of those who are cybersecurity savvy.

Phishing attacks and ransomware are the more common ways to get executives to provide the vital information needed to steal data

Understanding DoS and DDoS Attacks

Recently, A 23-year-old hacker from Utah who launched a series of DDoS attacks against multiple online services, websites, and online gaming companies between December 2013 and January 2014 was sentenced to 27 months in prison.

Austin Thompson, a.k.a. "DerpTroll," pledged guilty back in November 2018 after he admitted to being a part of DerpTrolling, a hacker group that was behind DDoS attacks against several major online gaming platforms including Electronic Arts' Origin service, Sony PlayStation network, and Valve Software's Steam during Christmas.

Ethical hacking involves testing to see if an organization's network is vulnerable to outside threats and Denial-of-service (DoS) attacks are one of the biggest threats out there. Being able to mitigate DoS attacks is one of the most desired skills for any IT security professional and is a key topic on the Certified Ethical Hacker exam.

According to US-CERT, Denial-of-Service (DoS) attacks occur when an attacker attempts to prevent legitimate users from accessing information or services. This is done by targeting a user system and its network connections, or the systems and network of the sites users are trying to use. An attacker may be able to deter other users from accessing critical healthcare assets on a website, system of even an entire network using Deauthentication attacks.

These attacks are commonly done when an attacker floods a network with information for example ack and syn-ack packets. To put this into a real-life scenario, when a user types a URL for a particular website into a browser, the user is sending a request to that site's computer server to view the page. An attacker can overload a server with numerous requests so that valid users cannot get through to the site. Also, an attacker can utilize spam email messages to flood a user's email account. For example, an attacker may send countless or large email messages to email accounts causing the users to consume their email quota and preventing them from receiving or sending emails.

Attackers use tools like hping3, hynae, LOIC, NTP (used for amplification), GoldenEyes, OWASP switchblade, BlackEnergy, among others. All these tools are open source and many come pre-installed as default in hacking operating systems. Ransomware is also a denial of service attack as it encrypts your data until you pay the ransom.

In a DDoS (Distributed Denial of Service) attack, an attacker may use one system to attack another system. For instance, the attacker may hijack or take control of a computer, forcing the computer to send out huge amounts of illegitimate data traffic to particular websites or send spam to particular email addresses. The attacker can also control multiple computers with malicious software (also known as botnets e.g. the Zeus Botnet) to launch a DoS attack.

It was reported on October 29th 2019, that one of the most popular torrent sites – The Pirate Bay had been put offline for almost a week due to a DoS attack. The attackers flooded The Pirate Bay with "searches that break the Sphinx search daemon," effectively crashing the torrent download website, making site visitors unable to download magnet links or torrent files. Sphinx is an open source full-text search engine, and The Pirate Bay reportedly used an older version of the software.

On October 23rd 2019, A team of German cybersecurity researchers has discovered a new cache poisoning attack against web caching systems that could be used by an attacker to force a targeted website into delivering error pages to most of its visitors instead of legitimate content or resources. Dubbed CPDoS, short for Cache Poisoned Denial of Service, the attack resides in the way intermediate CDN servers are incorrectly configured to cache web resources or pages with error responses returned by the origin server. The CPDoS attack threatens the availability of the web resources of a website just by sending a single HTTP request containing a malformed header.

DoS and DDoS attacks may escalate in the near future (as seen in the prior paragraph), especially with the increased usage of IoT (Internet of Things). IoT is a technology that allows multiple devices that have internet access to communicate and transmit data with each other through the internet, without the interaction of humans. This form of technology is used in the healthcare sector, energy sector, oil sector, cars, traffic lights, to mention but a few.

Protecting your organization from DoS attacks

There are a number of methods that can be used to defeat denial of service attacks, or at least to try. These come into one of two categories: mitigation through design and operational mitigation.

Mitigation through design includes establishing the capability for priority-based servicing, egress filtering, and ingress filtering. Operational mitigation includes IP address verification and dropping spoofed packets, rate limiting, understanding the characteristics of malicious traffic and dropping it, and understanding the characteristics of normal traffic and dropping anomalies. Priority-based servicing of traffic can be achieved by ensuring network traffic is marked with a priority attribute, and network queues are managed by priority.

To continue Visit;

https://www.forensicsinstitute.org/understanding-dos-and-ddos-attacks/

SIGHTS OF THE 2019 CYBERSECURITY AND RISK MANAGEMENT CONFERENCE