Cyber Security Trends to watch out in 2019

–**Nishtha Agarwal**,
Research Officer, Indian Institute of Public Administration, New Delhi, nishtha.5m93@gmail.com

While the world welcomes the Industrial Revolution 4.0 and the sophisticated technological environments along, the clever cyber crime arena has become an uninvited guest. It is no wrong to say that as the technology expands and develops, so do the sophistication of the ways in which cyber crimes are committed. Just like we protect our houses with newest equipments from clever thieves, cyber security is no different. Organisations also try to protect themselves from cyber criminals who are also armed with the newest technology that aid the organizations. Added to these are the growing concerns of stricter regulatory mandates like that of Aadhar and Personal Data Protection Bill to name a few which bring an ever pressing need to be on top of the IT security. This article discusses some of the cyber security trends that may affect Indian organizations in the ongoing year and which should be kept in mind to advance themselves one step ahead of cyber criminal.

The rapid changes in technology and evolution of Indian regulatory mandates put India into an interesting phase. Though the needs of India are not very different from that of the rest of the world, there are several areas which are unique to it and hence require different kind of attention. Following are some of the cyber security trends that Indian organizations should look forward to:

1. Targeted Phishing attacks: Phishing is a cybercrime in which the attacker contacts the target(s) via an email or phone or a text message posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords[1]. This information can be then leading to either an identity theft which in turn may cause financial loss. Unsuspecting users continue to fall prey taking bait from well-crafted business email compromise (BEC) attacks, phishing emails and malicious URLs. 2019 shall see this trend becoming more evident as hackers find phishing extremely lucrative to drop zero-day malware and ransomware threats through seemingly legitimate emails that may appear to come from trusted or familiar sources.

   As companies have trained their employees to identify phishing mails, the hackers have also increased their sophistication in creating these mails. Poorly constructed phishing emails are a thing of the past. Cyber criminals are able to launch highly localized, geo-targeted and personalized phishing threats.

What to do?

Businesses need to adopt comprehensive security awareness programs, which may include investing in phishing simulators that explain various emerging patterns or devious modus operandi of modern-day phishing attackers. This should help users identify and steer clear of suspicious phishing hooks, ensuring they do not end up handing over keys to the castle.

2. Privacy and personal data protection will be one of the key focus areas in 2019: With the draft Personal Data Protection Bill and the Aadhaar ruling by the Supreme Court recently limiting the use of data, the focus on data privacy will only increase in 2019. Organisations will invest in aligning their infrastructure to the requirements in the Personal Data Protection Bill (which is likely to become an Act later in 2019) to gain business edge and avoid penalties.

1 Retrieved from http://www.phishing.org/what-is-phishing , Accessed on April 26, 2019

What to do?

Organisations are advised to keep a close tab on the developments in the personal data protection bill and implement privacy and security by design in their processes.

3. Shadow inventory

An earlier prediction from Gartner warned that through 2020, a third of successful attacks will exploit shadow IT resources, meaning software programs and applications not approved by enterprise IT but still running on user devices. As businesses increasingly embrace software as a service (SaaS), BYOD (Bring Your Own Device) norms are also evolving and becoming somewhat lenient as users enjoy greater freedoms with their own devices. However organizations have to make sure that greater freedom to employees doesn't come at the cost of the organisation.

What to do?

To win in the race of digital transformation, businesses will need to develop enterprise wide cultures of security governance and constantly monitor user access rights and device permissions for possible irregularities[2].

4. Organisations will have renewed focus on cloud security in 2019: "Cloud" refers to the hosted resources delivered to a user via software. Cloud computing infrastructures—along with all the data being processed—are dynamic, scalable, and portable. Cloud environments are highly connected, making it easier for traffic to bypass traditional perimeter defenses. Insecure application programming interfaces (APIs), weak identity and credentials management, account hijacks, and malicious insiders may pose threats to the system and data.

What to do?

As cloud adoption continues to grow in 2019, attacks on cloud's shared security model will mount manifold. Cloud providers will have to put in more resources to protect infrastructure. Technologies like Cloud Access Security Broker (CASB)[3] which comes with additional security controls should be adopted. It is a software tool which is present between the organisation's on-premise infrastructure and a cloud service provider infrastructure. It allows the organization to extend the reach of their security policy beyond their infrastructure. This is done by making sure that the network traffic between on-premise devices and the cloud provider complies with the organisation's security policy. It gives the insights into cloud application use across cloud platforms and identity unsanctioned use.

Along with increased deployment of resources, efforts should be done to increase understanding about how to limit access to data stored in cloud and let only authorised personnel access it.

Besides this, as mentioned earlier, security by design should be followed by organizations. Preventing unauthorized access in the cloud requires shifting to a data-centric approach to encryption of the data. Strengthening of the authorization process along with strong passwords that have 2 factor authentications should be used.

Conclusion

We see that the cyber arena is ripe with threats that are advancing at almost the same rate as the arena is. The more the innovations, the more security holes hackers are able to find. Black hat hackers are becoming smarter than ever before. Keeping up the pace with technology along with cyber security trends is essential. This will help to defend well against cyber security attacks. The main solution that comes out of this discussion is the incorporation of privacy by design and security of design. Business leaders are recognising that cybersecurity must be aligned to their overall business goals and, moreover, that they must be cybersecurity-conscious at every point in their digital transformation journey. Cybersecurity is being built-in as technologies and applications are conceptualised, designed, adopted, and built. DevOps and security operations teams are beginning to work more closely – as a DevSecOps team – creating the tools that enable secure digital transformation.

2 Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/02/07/five-cybersecurity-trends-to-watch-for-in-2019/#399250cf4c66 Accessed on April 26, 2019

3 Retrieved from https://searchcloudsecurity.techtarget.com/definition/cloud-access-security-brokers-CABs, Accessed on April 26, 2019

Ms. Nishtha Agarwal, Research Officer, Indian Institute of Public Administration, New Delhi.

nishtha.5m93@gmail.com