VOLUME XIV ISSUE 7
JULY 2023
OTTAWA ON

Emerging Threats and Trends of Cyber Security

Cybersecurity is a growing sector. As a hacker or security provider, you should learn about the emerging threats and trends of cyber security. These new threats and innovative trends can give you new ways to combat them.

This article will summarize all the threats and trends of cyber security. Read this article to learn them and utilize them in your daily life.

Trends and Threats of CyberSecurity

Following are some of the latest trends and threats to cyber security. These are:

Remote Working Cyber Security

After COVID-19, most organizations shifted their work mode to remote or online. Remote working brings out new concepts and risks of cyber security. Moreover, it is one of the most discussed trends these days.

We all know that a home office is less protected than a centralized office. This means remote working has less secure firewalls, fire management, and routers. Remote workers usually forget the security vetting in a rush to keep things operational and managed. Cybercriminals can take advantage of it.

Rise of Ransomware

Ransomware isn't a new threat to cyber security, but it is growing faster now. It has been estimated that more than a hundred ransomware families and hackers have hideous malicious code.

It is an easy way for hackers to gain all the financial rewards. Remote working is one of the reasons behind it. It resulted in the new targets of ransomware with increased attacks.

Elevated Cloud Services and Cloud Security Threats

One of the most important trends in the cyber security business is still cloud vulnerability. Once more, the broad adoption of remote work in the wake of the epidemic has dramatically raised the need for cloud-based services and infrastructure, with security implications for businesses.

Usually, cloud services offer a wide range of benefits. But they are also the main target of the hackers. But why so? Misconfigured cloud setting is a primary cause of breaches in data and its unauthorized access, along with account hijacking.

Social Engineering

Social engineering is one of the top most dangerous threats to cyber security. Cybercriminals have been using this technique for over a decade. This technique relies on human error rather than any technical vulnerabilities.

This technique can easily trick humans and benefit its users. It can easily cause a breach in your security system and causes harm to it.

Third-Party Exposure

Cybercriminals usually prefer less-protected networks that belong to third parties. It is for them to get access to such a network. This trend is always emerging in cyber security. Hackers can also leak the personal data of such networks.

Ethical Hacking - Why is it Important

Ethical hacking means a good hacker with authorized access to your system or data. Ethical hacking is used to secure the critical data of any organization. Moreover, it helps to understand the behavior of malicious attackers and hackers.

Ethical hacking attempts to secure the flaws and faults of an organization's security system. They discover them and solve them as soon as possible before the malicious hackers. People usually wonder what is even important. Read this article to find out.

Importance of Ethical Hacking

Some key points show the importance of ethical hacking in any organization. They are:

- It keeps the organization out of the trouble caused y hackers.
- It prevents the damage or stealing of important data
- It avoids security breaches
- It can gain the trust of clients and customers
- It repairs the entry points to avoid a crisis.

Undoubtedly, ethical hacking provides quality assurance of tools and procedures. It instantly detects and eradicates the flaws of the system. We hope this article will make you understand the importance of ethical hacking in any system.

What is Digital Agility

Digital Agility is the ease with which an organization can rapidly enable, update, change, or adapt their processes. With digital agility, you can improve cross-departmental collaboration. Below are some popular uses of digital agility to improve productivity:

1. Empower your employees with easy-to-understand and simple tools. This will motivate them, improve their skills, and enhance their abilities.
2. With digital agility tools, your employees can save time when solving problems. These tools include an easy-to-use interface for your employees.
3. Your employees will easily understand the tool without any need for training sessions.
4. You can easily integrate these tools with third-party plug-ins, thereby increasing productivity.

Secure Your Cloud Data through Encryption

Encryption is the best way to protect your data. Only a person with the password can open the file. No one can see the content of the file after you move it to your Cloud system. Here are some tips that you can follow to secure your important data in Cloud with the help of encryption:

- Encrypt your data before uploading
- Secure the access by cloud cryptography
- Protect your data while in transit or at rest with the help of Cloud Access Security Broker.
- Locally back-up the data in your cloud system
- Use encryption with the help of your cloud service provider

What is the Future of Cyber Security

The industry is revolutionizing with the increase of cyber threats. But some evolving tools can defend this system and make this complex network much easier for its users. Some predictions are made by experts related to the future of cyber security. Read this article to learn about them.

Future of Cyber Security

You will be able to work from anywhere permanently. This means that you don't have to visit your workplace. Technology will allow you to have all the firewalls and best security access to protect your system. Everything will be automated. This will reduce the chance of error. It will solve all the problems and threats that increasingly endanger the complex web of computing resources. There will be the adoption of zero-trust principles. The future of cyber security is extremely bright and useful for the next generation. However, some amendments can make cyber security an error-free system in the future.

Take the NeoLore Cyber Security Survey

Has your company done a Cyber Security Maturity Assessment within the last year? Do you have an IT security policy in place? Do you know if you've been hacked or are leaking data?

If your answer was "no" or "I'm not sure" to any of those questions, your company may be at risk for a devastating cyberattack.

Get the NeoLore Networks Cyber Security eBook for Free!

It Features

- Information on the various threats to your business
- NIST Security Framework
- CIS Controls
- Basic Controls

And More!