What are the biggest security threats to local/state government?

Nasrumminallah Zeeshan

(B2B/IT Freelance Writer)

In today's world, cyber threats have been emerged as routine challenges in our daily life.

They are confidently affecting government infrastructure, and make us think about taking solid actions to avoid them.

But before we apply any policy, we will need to know and identify them first.

This situation causes many problems which require constant dealing for obtaining the expected results with technical systems.

This article contains the biggest security threats faced by government along with their trendy solutions. We will also discuss about specific regulations, policies and standards need to be considered.

1. Threats by Technology Trends

It was 1950s, when the Internet came into being. At the start, the Internet served the people with a simple infrastructure of internal laboratory computers, but as it continued expanding with the passage of time, it became one of the most complex structures of inter-connected computer networks.

The Internet device manufacturer Cisco confirms the sale of 49.25B annually. They also periodically announce security fixes in their devices which needs immediate actions by security professionals in charge.

Policies, Standards and Regulations need to be considered

- **Policy:** Government needs to create a security testing response routine like Google. They will ensure to test and find out security weaknesses in infrastructural devices prior to implement them on mass basis.
- **Standards:** Government must avoid allowing insecure technical infrastructure and ensure to check the standard of systems with a solid security benchmark set.
- **Regulations:** Government must regulate security testing on timely basis. They must officially confirm periodical security testing as a rule for better

information security. In this example of Facebook, we can see how they use technical experts to test and validate their system's security.

2. Physical Threats

According to Your Business, the ratio of affection by internal factors has been increased significantly in recent years.

Physical threats include the internal factors having affected on a government institution or systematic structure. These factors include government institutions, employees, technical failures, implementation of bad policies and natural disasters.

Policies, Standards and Regulations need to be considered

- **Policy:** Government needs to focus on enquiring professional man power as well as technical infrastructure satisfying a predefined set of quality benchmarks. This example of real world professionals highlights the need of the said factor.
- **Standards:** An official infrastructure must ensure following a solid strategy to carry out routine tasks. Government needs create a basic checklist for every task being completed in an official environment. Mashable illustrates the Facebook's security precautions for end users.
- **Regulations:** Government needs to focus on creating a central monitoring system like USA implements. This ensures to have an eye on routine things and fix the gap when necessary.

3. Cyber Crime

More than 38% cyber crime incidents have been increased in 2015, according to PWC report.

As official assets are being prioritized for automation, government faces immense challenge of detecting, tracking down and controlling the cyber crime against their online assets.

Policies, Standards and Regulations need to be considered

- **Policy:** Yahoo has successfully controlled the cyber crime by implementing the policy of creating country level gateways. Gateways are centralized bridges for detecting unwanted requests and take them down if not satisfying a predefined list of security benchmarks.
- **Standards:** There should be a list of objectionable content requests. The Government needs to check each incoming request against a list of objectionable content list and handle it the way suitable according to security measures.
- **Regulations:** Google Search Algorithm confirms the effectiveness of automation. If the government creates automated systems for validating routine integrity, the cyber crime ratio can efficiently be reduced.

4. Network Visibility

According to Shodan, there are billions of devices connected online each single day.

The Internet is a collection of inter connected networks of computers. When an official system is connected to the Internet, it becomes a part of large networks easily discoverable online.

The government needs to hide their sensitive network infrastructure. It is mandatory to stay safe from network level attacks including DoSS attacks, dictionary attacks, brute force attacks, request forgery and phishing attacks.

Policies, Standards and Regulations need to be considered

- **Policy:** Government must create a policy about their sensitive infrastructure online. They need to implement a policy consists of deciding about their network exposure online, maintaining security precautions of already connected systems and controlling real time threats by creating a team of emergency response. A better example of suitable privacy is shown by Google Privacy Policy.

- **Standards:** F-Secure confirm the real world example of implementing and controlling network visibility precautions. The world's top companies like Google, Yahoo, Microsoft and Facebook are constantly using Apache Web Server rules to control their network visibility.
- **Regulations:** Government needs to hire the professional community. They can be hired for making customized tools to test, detect, check and control real world scenarios.

5. Backdoors

Backdoors are known as the popular way of compromising security. These are special tools to steal sensitive data and send it back to its original author.

According to Symantec, there are more than **1,122,311** backdoors are currently wandering online.

To avoid stealing sensitive information, Virus Total methods are real world examples of checking routine factors for hidden backdoors.

Policies, Standards and Regulations need to be considered

- **Policy:** Government can implement the policy of tracking down affected software by building a strong antivirus system as a main testing gateway. Government also needs to carry on security research for hunting and tracking down newly created backdoors.
- **Standards:** It is mandatory to force follow a specific security checklist for government infrastructure. An example of how Google deals with mail attachments is the implementation of Norton antivirus on their testing systems.
- **Regulations:** Government must scan official records and documents on regular basis. If certain automated systems like National Vulnerability Database are built, government can take down backdoor viruses trying to steal sensitive official information.

6. Staff Training

The man-power in organizations play important role in overall security. There are the hacking methods like Social Engineering, consisting triggering human behavior to carry out specific security compromises.

To avoid hackers exploiting technical human weaknesses, the government needs to educate people according to security standards. An example of this incident confirms how hackers got sensitive information by exploiting human weaknesses.

Policies, Standards and Regulations need to be considered

- **Policy:** Government needs to implement policy for carrying out official training programs. It is important to educate people for technology and prevent incident like Jdsupra discusses.
- **Standards:** The Government is subjected to keep qualified people in charge. They must also ensure to test and improve their man power on periodic routine.
- **Regulations:** It is important to hand over specific security checklists to each individual. If the routine tasks are carried out according to specific security benchmarks, the government is expected to carry out smooth security measures.

Conclusion

In order to deal the trendy security threats in today's world, the government must focus on dealing technical infrastructure according to security benchmarks as well as educate human resource accordingly. The government is also subjected to make and implement specific policies, execute security precautions on timely basis and create automated systems to obtain results in fast manner.

References

- **Cisco** - http://www.marketwatch.com/investing/stock/csco/financials
- **Google** - https://www.google.com/about/appsecurity/learning/xss/
- **Facebook** - https://www.facebook.com/whitehat
- **Your Business** - http://yourbusiness.azcentral.com/internal-external-factors-affect-organization-11641.html
- **Freelancer** – http://www.freelancer.com/
- **Mashable** - http://mashable.com/2016/11/29/facebook-privacy-checkup/
- **USA Central Station** - http://usacentralstation.com/
- **PWC** - http://www.pwc.com/gsiss
- **Yahoo** - http://finance.yahoo.com/news/skyhigh-networks-recognized-leader-cloud-215100161.html
- **Google** - https://www.google.com/insidesearch/howsearchworks/algorithms.html
- **Shodan** - https://www.shodan.io/
- **Google Privacy Policy** - https://www.google.com/policies/privacy/
- **F-secure** - https://sense.f-secure.com/
- **Apache Web Server** - http://www.tecmint.com/apache-security-tips/
- **Symantec** - https://www.symantec.com/
- **Virus Total** - https://www.virustotal.com/
- **Norton** - https://us.norton.com/
- **National Vulnerability Database** - https://nvd.nist.gov/
- **Wikipedia** - https://en.wikipedia.org/wiki/Social_engineering_(security)
- **Information Security Institute** - http://resources.infosecinstitute.com/social-engineering-a-hacking-story/
- **Jdsupra** - http://www.jdsupra.com/topics/data-breach/employer-liability-issues/