Securing your work place from cyber-attack and global best practices

MD SABBIR HOSSAIN

Recent cybercrime incidents have shown that even government networks are not safe from attack. In principle, these should be even better secured than normal company networks, but professional hackers have often managed to penetrate these systems in the past. The Bundestag was attacked in 2015. Companies are increasingly becoming the target of hackers against the backdrop of industrial espionage. The previous measures against these attacks are definitely not yet adequate and preventive. The aim of every company should be to act instead of react. In most cases, companies are rigorously surprised by attacks, if they even notice. Against this background, firewalls only help to protect one's own systems to a limited extent. Because, above all, complex infrastructures can only be protected with a great deal of security, a large number of measures and security-relevant technologies. The human factor also plays an important role. Most systems are connected to the Internet, where employees have to answer emails or open attachments.

Cyber-attacks are the de facto threat today. The increasing volume of data and the openness of the networks harbors dangers, because everyone uses smartphones, tablets, computers and other networked devices in everyday business. All of these devices are connected to the Internet and are therefore potential gateways for attackers to break into the entire company network. For the management level, the question arises: what threat scenarios are there, what damage can be expected to your own organization and how can companies protect themselves? With 220 million suspicious activities taking place on the networks every day, according to NATO, decision-makers often need even better information about the threat and the types of cyber-attacks.

At the moment, IT security has little perception in companies. The high degree of networking and the simultaneous exchange of company-critical data via the Internet offer cyber criminals greater potential than ever before. This is a big problem that companies have to adapt to today and in the future. Because, above all, data from the R&D, marketing, human resources and finance departments are in great demand. According to this, cyber criminals are particularly interested in customer and employee data, balance sheets or even access to bank accounts.

But what types of attacks do cyber criminals attempt to get into company systems? A list of the types of attacks is intended to give company decision-makers an overview of which attacks they should expect:

- Ransomware
- DDoS
- Phishing
- Botnet
- Insider Threat
- Malware
- APT etc.

These types of attack are defined by different attack vectors and type families with which cyber criminals attempt to break into company networks or infrastructures. These attack vectors are combinations of attack methods and techniques that a cybercriminal can use to gain access to IT systems.

These attack vectors include, for example, spam attempts that are sent by means of unwanted messages that are sent through targeted and untargeted via e-mail or other communication channels. In addition to unwanted advertising information, these messages primarily contain links to infected websites or attachments. Against this background, spam emails are also used for phishing attacks.

In addition to the common spam e-mails, cyber criminals try to locate weak points within the company's servers primarily with targeted attacks, because if systems are only equipped with inadequate firewalls, it is often easy for hackers.

Drive by exploit kits are also an important tool used by cyber criminals. With this attack vector, cyber criminals attempt to find security gaps on a computer by means of automated exploitation. Above all, users who are on a website are observed. Without further user interaction, the hacker tries to locate and exploit weak points in the web browser, in additional programs of the browser (plugins) or in the operating system of the user in order to implant malware unnoticed on the user's computer.

If your own company has been the victim of an attack, the specific extent of the damage depends to a large extent on the technical and organizational measures (TOMs) that have been taken to prevent the attack either preventively or detectively. Even if preventive measures could not prevent the attack, in the event of an attack detection measures and a quick response from the security organization can ensure that the damage is limited.

But what are the typical damages that companies can expect as a result of a cyber-attack?

In addition to the monetary aspects, in the form of compensation and damage to the company's image, industrial

espionage is a major issue. Accordingly, this can be self-damage, in which the consequences of a cyber-attack mean the failure of production or services and thus high costs result from impairments or production interruptions.

In addition, damage to the company's image or reputation is a problem. In the event of an attack, companies often lose a good reputation with customers and may have to plan new budget for advertising campaigns in order to polish their image again.

As a rule, companies also have to pay compensation if they breached their legal or contractual obligations towards third parties as a result of an attack. These compensation payments can turn out to be very high, especially for systems and infrastructures that store a large amount of business-critical data.

The general best practices for companies include a large number of preventives, detective and reactive TOMs that know how to prevent infection from cyber-attacks or minimize the risk of attacks. These measures are particularly up-to-date given the number of targeted threat scenarios.

Preventive measures primarily serve to protect one's own systems and infrastructures from the attack vectors mentioned above. This includes protective measures for client systems that prohibit the execution of script files and guarantee protection on mail servers, through blocking or quarantine. In addition, various patch management applications that run on client systems can protect against drive-by attacks. The secure use of web servers also significantly reduces the attack surface.

In addition, preventive measures include sophisticated data security concepts and backups that still ensure the availability of the data in the event of an attack.

Raising employees' awareness plays another important role. Awareness can be created through training courses and campaigns and your own employees know how to take care of IT security and what to do in the event of a spam email or a social engineer attack.

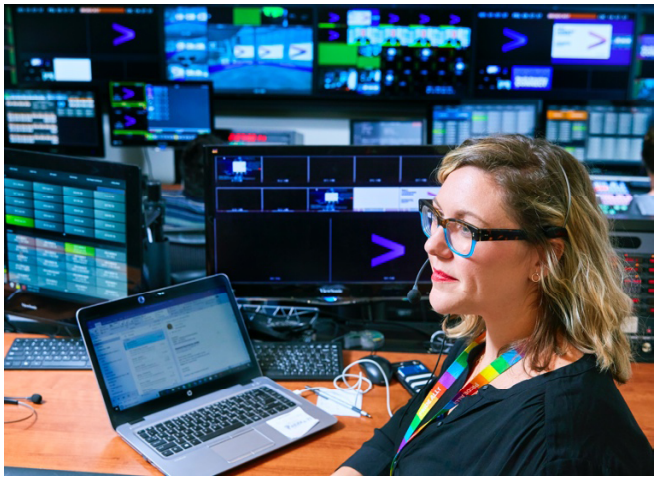
In addition, secure administrator accounts, a precise definition of data types that may be stored on servers, and firewalls also serve to protect against infections.

In addition to preventive measures, detection measures (e.g. intrusion detection with automatic notification of the relevant people) may also be necessary in order to, in the event of an attack, evaluate log data that can determine the size of the attack and also identify ways in which these attacks are the company arrived.

Regular network monitoring can also check the interfaces between the server and the gateway and block possible attacks.

However, in the event of an attack that circumvented all preventive measures, the security organization should act quickly. These can be various technologies, the primary goal of which is to prevent damage, to guarantee the isolation of the infrastructures and systems and to ensure normal operation. It should be noted that a combination of preventive and reactive measures ensure that the attacked systems withstand. So no "either / or decision" - but only through this combination a high level of security arises within the company, which detects attacks and reacts quickly in the event of an attack in which preventive measures have been circumvented and tries to neutralize attacks and also quickly generates a report / Can send log to your own security organization These technologies can be:

- Identity Access Management
- Antivirus



- Anti-malware and spyware
- Intrusion detection and prevention
- Next generation firewall
- Security information and event management
- Mobile device management
- Vulnerability Management
- Web application firewall
- DDoS protection
- Device control
- Data loss prevention
- Encryption
- Anti-spam
- Web filtering

Another measure against cyber-attacks can also be as a company to commission the hackers to attack their systems. The aim of the company's own hackers is to find the gaps in the systems before others can exploit them. Various service providers offer their resources in this context and support companies in closing the security gaps. For years, many companies lacked the awareness and competence to react appropriately to the threat from the Internet.

A large number of IT decision-makers and CISOs do not yet know which strategy is the right one to counter cyberattacks or which measures and technologies are to be used against them. In order to advance the mindset and the IT security concept in the company, IT security and data protection should be practiced from the ground up and the risk of cyber-attacks should be minimized at every workplace and taken into account in the system design. Whenever new systems are built, think about security and data protection right from the start (security by design, privacy by design). Thus, infrastructures are given a certain security impact from the ground up. Against this background, external service providers in particular can support companies with their expertise and stand by as sparring partners.

Writer Bio: A security professional with over 9 years of experience in security consultation, security design, Framework Design, Policy Making, project development and execution, integration of various technologies, lawful interception system, OSINT, Digital Forensics, Cell interrogation & active tracking system, critical infrastructure security, tactical & intelligence solutions. He is currently employed in BGD e-GOV CIRT (Bangladesh National CERT) as well as pursuing his Masters Degree from University of Ottawa CJ

Feedback: sabbir.hossain@cirt.gov.bd