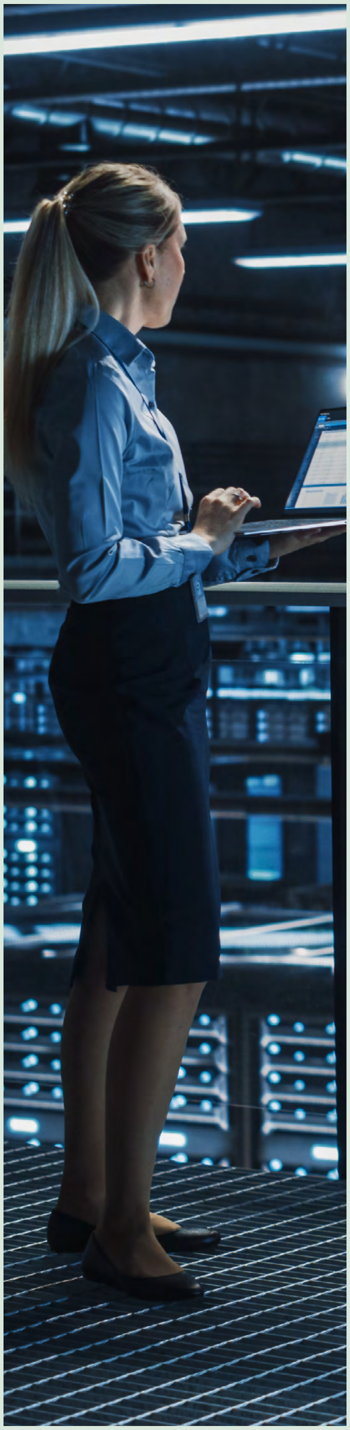
WHITE PAPER



CYBERSECURITY DILEMMAS - HOW SHOULD CHINESE COMPANIES COMPREHEND AND ADDRESS ISSUES

Abstract

Currently enterprises in China are actively engaged in digital transformation, during which information security issues bring a common dilemma - the need to handle security threats and conform to national information security regulations and, the impact on user experience, complexity, IT and operational efficiency, cost, time to market, etc. It is important for organizations to decipher how best they can solve this problem.

Cybersecurity risks jeopardize an enterprises strategic objectives, business continuity, business transformation targets, service quality, personal and business data protection, customer churn, service availability, service levels, reputations, and other aspects due to non-compliance. These risks are present at every level of the enterprise architecture. This paper focuses on security issues faced by Chinese enterprises, the principles of various threats, requirement of security regulations, and the perspective of organization-specific risks and compliance requirements faced by enterprises. Read this whitepaper to get a better understanding of information security issues, reducing the risks, making informed decisions and achieving a balance between costs and benefits.

Infosys®
Navigate your next

Industry Overview

There is a growing need for designing enterprise security architectures from a holistic perspective. Enterprises vary in size, complexity, business environments, level of maturity and challenges being faced. As a result, it is necessary to choose a diverse path among many short, medium and long-term goals. Cybersecurity in an enterprise mostly constitutes of risk management, risk identifications and lifecycle management. The countermeasures include business, information, technology architectures and solutions.

However, at one hand, the risks need to be mitigated, at the other hand, the decisions, priorities, sequence, and evaluation of investments often register a high level of inefficiency and may create issues such as availability of services and better user experience.

Solution

We recommend an enterprise architecture design approach that can improve the overall design of the security architecture.

The advantages of this method are:

1. Better accuracy to identify solutions to address enterprise specific issues
2. Clearer visibility of enterprise level transformation projects to avoid redundancy
3. Holistic security architecture to optimize the development and maintenance of security solutions.

Designing the enterprise level security architecture means:

1. Comprehensively define the business strategy, business driving force
2. Correctly define the vision to be achieved by the enterprise security architecture
3. Gradually implement security solutions at the business and IT architecture levels (refer to TOGAF 9 for the description of the architecture design approach ADM).

Article 2, "Properly defining the vision to be achieved by an enterprise security architecture is a core step in connecting the ladder."

In the following, we examine security regulations and requirements to help you better define the right security architecture and make recommendations at the solution level.

Part 1: Regulatory compliance requirements and the countermeasures

While an individual industry or enterprise focuses its own business interests, China authorities intend to maintain information security across industries and all citizens. China has established a basic legal compliance framework for cybersecurity. It requires enterprises to strengthen the capability of security compliance and fulfill their own statutory compliance obligations, failing which, they would experience business losses of different levels.

These are the three major regulations:

1. The Cybersecurity Law Of The People's Republic Of China.
2. The Data Security Law Of The People's Republic Of China.
3. The Personal Information Protection Law Of The People's Republic Of China (Or PIPL).

Government authorities, such as the Cyberspace Administration of China ("CAC"), have issued various regulations to implement the "Three Basic Laws." In addition, other government, and semi-government agencies, such as China's National Information Security Standardization Technical Committee("TC260"), have also released many national standards for detailed guidance.

The compliance of an enterprise involves multiple departments. It is necessary for the enterprise to identify all the related departments appropriately.

To be compliant, enterprises need to implement measures such as MLPS, personal information Protection, Risk Assessment, Daily Monitoring, Data Cross-Border Assessment, Network Security Review etc. Among all, MLPS and Outbound Data Transfer has created a major impact in China.

1. MLPS requirement and practice

As a normative document, Multi-Level Protection Scheme (or "MLPS"), refers to the implementation of graded security protection for information systems that store, transmit, and process information.

According to the CyberSecurity Law of China, all information operators are required to fulfill the obligations under MLPS, including level determination and assessment. Failure to carry out MLPS is violation of the law.

The technical framework of MLPS can be summarized as "One Center, Triple Protection", where "One Center" refers to the secured management center, and "Triple Protection" refers to secured communication network, zone boundary, and computing environment, which forms the MLPS framework.

MLPS has five levels, and the higher the level, the stricter the requirements are. But the majority of the enterprises are more related to Level 2 and Level 3.

Infosys recommends five steps to deal with MPLS:

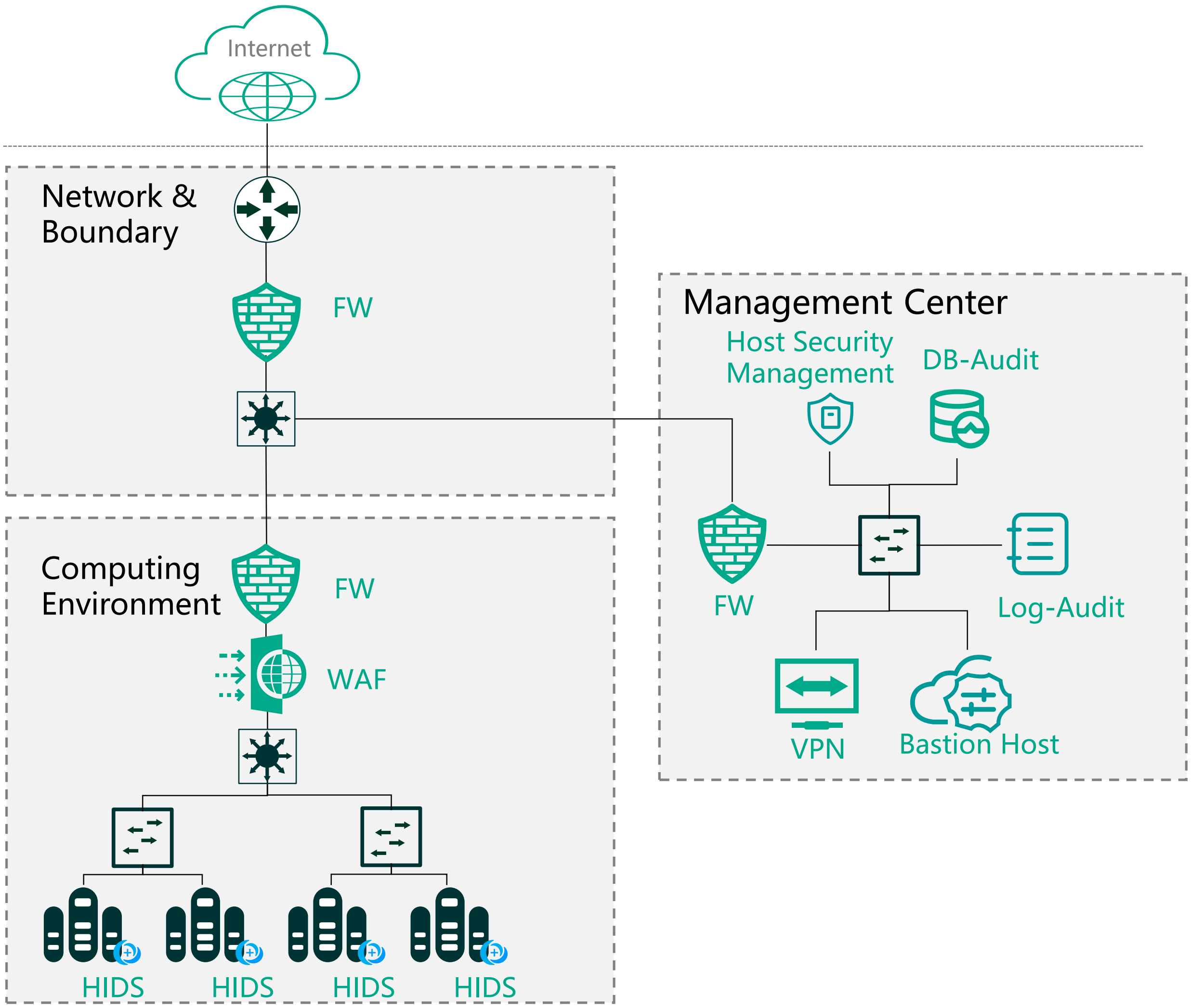
1. **Determine the security level**

Enterprises are responsible to determine their own information system's MLPS level based on the degree of damage (if the system is destroyed). The public security department reviews the level and notifies.

Level-2 or higher-level information systems must: (i) review the rationality of the determination; (ii) obtain the approval from the competent industry authority (if any); and (iii) file the result to the public security authority for review.

Below diagram depicts the technical solution example for the MLPS Level 2.

Figure 1. Technical solution for MLPS level 2



2. **File recordation form**

The enterprise must fill in the "MLPS Recordation Form" and a series of other materials and submit them to the public security for recordation review.

3. **Enterprise security buildup and rectification**

The enterprise must conduct Investigation, Gap Analysis & Reformation Plan, rectification & system security reinforcement and identify unsafe factors for rectification.

4. **Evaluation and assessment**

The enterprise must approach an evaluation agency to conduct a comprehensive evaluation, get a qualified evaluation report and pass the certification.

5. **Supervision and inspection**

The public security organizations supervise and inspect the protection work and issues the record certificate.

In most cases, obtaining a MLPS certification can give an enterprise enough security level.

Table 1. Technical products for MLPS level 2

Category	Content	Requirement
Host Security	Meet the MLPS requirements of secure computing environment	Must
Security Management Center	Meet the MLPS requirements of security management center	Must
Firewall	Meet the MLPS requirements of secure communication network and secure zone boundary	Must
O&M Audit (Bastion Host)	Authentication, operational auditing, access control	Optional
Web Application Firewall (WAF)	Application security	Optional
VPN	Meet the requirements of remote access transmission security	Optional

Below diagram depicts the technical solution example for the MLPS Level 3.

Figure 2. Technical solution for MLPS level 3

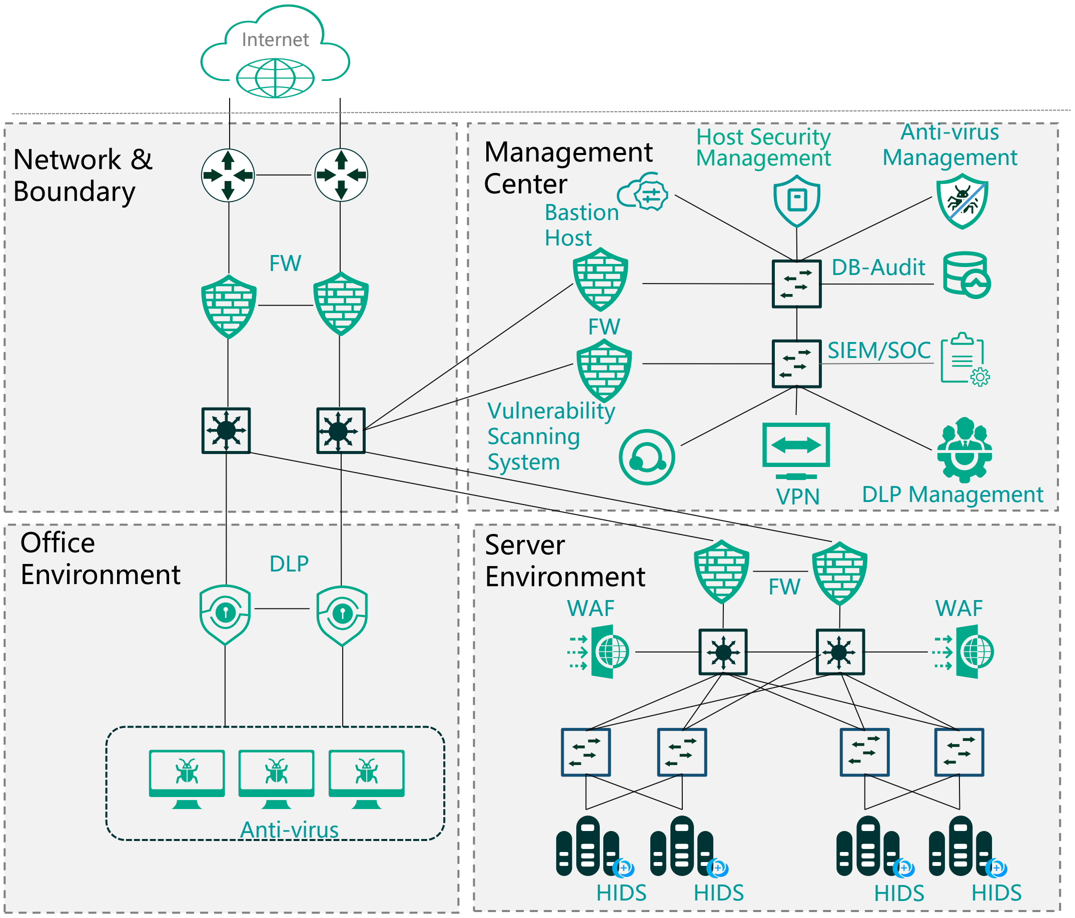


Table 2. Technical products for MLPS level 3

Category	Content	Requirement
Host Security	Meet the MLPS requirements of secure computing environment	Must
Security Management Center	Meet the MLPS requirements of security management center	Must
Firewall	Meet the MLPS requirements of secure communication network and secure zone boundary	Must
O&M Audit (Bastion Host)	Authentication, operational auditing, access control	Must
Web Application Firewall (WAF)	Application security	Must
Vulnerability Scanning System	Discover and manage known vulnerabilities	Must
DB-audit	Meet application and data security requirements	Must
VPN	Meet the requirements of remote access transmission security	Optional
DLP	Data leak protection	Optional

2. Outbound data transfer requirements and practice

Under the Data Security Law, "data" includes not only electronic data, but also data recorded or stored in non-electronic forms (such as data recorded in paper files).

"Important data" is defined as data in a specific field, specific group, specific region, or data that has reached a certain level of accuracy and scale. Once leaked, tampered with, or damaged, it may directly endanger national security, economic operations, social stability, and public health and security.

"Personal information" refers to the identified or identifiable data recorded electronically or by other means but excluding anonymized information.

"Sensitive personal information" includes biometrics, religious belief, specific identity, medical health status, financial accounts, and the person's whereabouts, as well as the personal information of a minor under the age of 14 years.

Most enterprises in China only protect "personal information" while "important data" mostly occurs in Critical Information Infrastructure (or "CII").

For those companies owning large amount of personal data (clients, partners, and internal employees etc.), cross-border transfer of those data without protection might breach the PIPL. To be compliant one should:

1. Pass the security assessment organized by CAC
2. Obtain personal information protection certification issued by professional organization/agency

Table 3. Three major mechanisms for outbound transfer of personal information

Execution time	Issued Agency	Name	Abbreviation
6/1/2023	CAC	Measures for standard contracts for outbound transfer of personal information	Standard Contracts
12/16/2022	TC260	Practice guidelines for cybersecurity standards - Security certification specifications for cross-border processing of personal information V2.0	Security Certification
9/1/2022	CAC	Security assessment measures for outbound data transfer	Security Assessment Measures

3. Sign a standard data protection contract with the receiver
   Here is the general information about the three compliance mechanisms.

It is recommended that enterprises follow the "two-step" principle:

Step 1: Identify statutory trigger scenarios

Use architecture artefacts to find out the scenarios where outbound transferring of personal data are required. To be certain, it might be necessary to exploit formal assessment.

Step 2: Choose the applicable data cross-border transfer mechanism

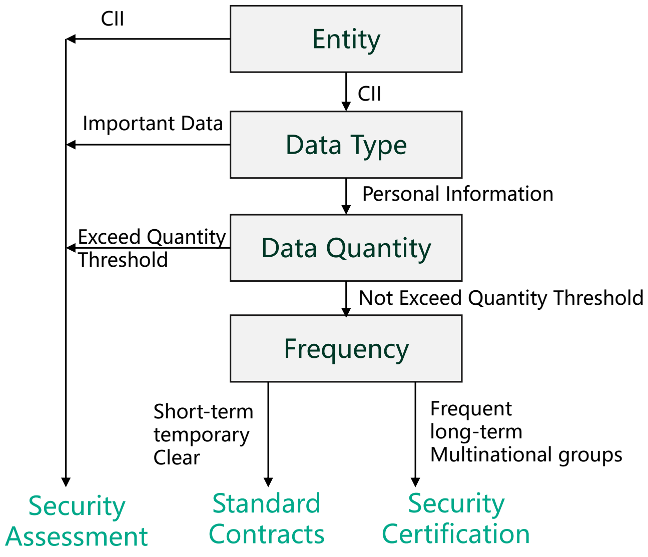
If the security assessment of the declaration is not triggered, the enterprise can conclude standard contract or obtain personal information protection certification based on the business activities and data conditions.

For short-term and temporary cross-border transfer of personal information, or with clear scenarios in cross-border transactions, the "Standard Contract" has the advantages of efficiency and low cost.

For the cross-border transfer between affiliated companies of the group, it is easier to formulate and follow unified rules for the cross-border processing of personal information, and it is better to use "Security Certification."

"CII" refers to "Critical Information Infrastructure," and "Quantity Threshold" refers to "Process personal information of more than 1 million individuals or cumulatively transfer personal information of 100000+ individuals or cumulatively transfer sensitive personal information of 10000+ individuals from Jan 01 of the previous year".

Figure 3. Outbound data transfer paths



Part 2: Types of security threats in China and the countermeasures

The three most frequent threats - DDoS, ransomware, and data leakage are increasing in volume (e.g., DDoS is now reaching TBPS) and sophistication. They are mostly profit driven (e.g., ransomware keep evolving which even leads to the emerge of ransomware-as-a-service, or RaaS). Data leakage is drawing more attention because most business functions, architects and IT operation keep seeing the risk in their solutions and operations.

It was observed that one single cyber security incident can reach millions of dollars, and this trend is still going up.

It is worth noticing that since digital transformation require the change or adoption of increasingly human-machine interactions, more application integrations, more data transferring, more migrations, it leads to vulnerabilities and reshapes the IT architecture and the way business is using the IT tools. The more digital technologies are adopted, the more threats become reality.

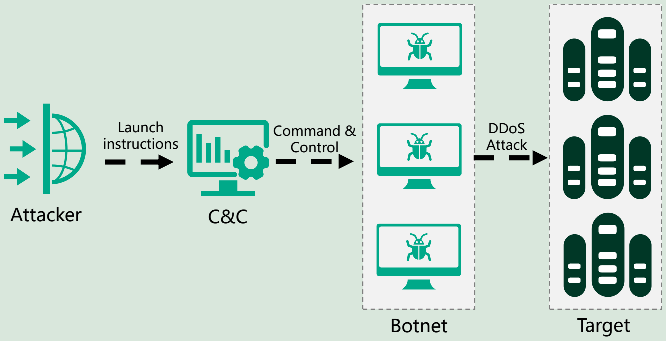
Threat 1: Distributed Denial of Service, or DDoS

As one of the serious threats to cyber security, DDoS has been active for more than 20 years. It occurs frequently, and it is continuously adapting.

A DDoS attack refers to multiple (often numerous) attackers in different locations attacking one or several targets at the same time. In many cases, these 'attackers' are also victims whose computers are infected by malware and controlled by a team of attackers. These attacks look like normal IP, TCP, or other payloads of transactions, but because they happen at the same time and in volumes higher than the target systems can handle, the victims are unable to respond to significant business requests, and the users would experience no response at all.

A complete DDoS attack requires four types of participants: attacker, Command and Control Server ("C&C"), botnet, and target. The attacker host launches attack instructions, directs C&C and botnet to launch DDoS attacks. The C&C helps to hide the attacker. The botnet directly attacks victims by sending large volume of attacking traffic. The botnet is based on PC at the beginning and eventually on a variety of wireless devices including smart phones and IoT.

Figure 4. DDoS attack process



The way botnet launches attacks adds its complexity - there are two main methods: "traffic attack", which is mainly aimed at consuming up network bandwidth by flooding packages; "resource exhaustion attack", on the other hand, uses up host's memory and processes (e.g., by setting up numerous incomplete TCP sessions), resulting in the inability to provide services.

According to the analysis of the "DDoS Attack Threat Report for the First Half of 2022", in China, the DDoS attack situation is:

- The number of DDoS attacks in the first half of 2022 reached a four-year high, three times that of the same period in 2021. The game and video industries rank top two among all the victims.
- Tb-level attacks occurred for three consecutive months, and hundreds of Gb-level attacks exceeded 40 times a day on average.
- 70% of the attacks lasted less than 30 minutes, and 35% of the attacks lasted less than 5 minutes.

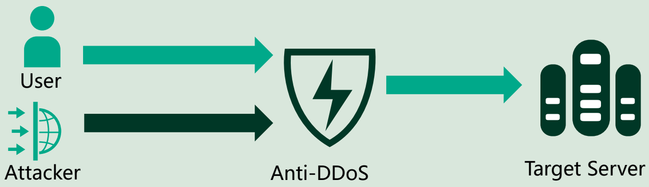
- While traditional attacks (e.g., UDP reflection and large SYN packets) remain stable because of the growth of defender capability, new types (such as TCP reflection and PSHACK) continue to increase because they're more difficult to defend.

DDoS attacks are becoming more complex, more extensive, and cheaper, which makes the industries to keep developing anti-DDoS counter measures in China:

- Increase network equipment performance - The fundamental way to fight against DDoS is to increase the throughput capability of routers, switches, firewalls etc. This is true for ISPs, cloud operators and rest of the world.
- Increase servers' security level - Security measures such as vulnerabilities scanning, timely patching, suppressing unused services and ports, etc., to reduce the risk of servers exploited due to DDoS attacks.
- Buy services from operators to bypass attacks (such as Distributed Cluster Defense) – It is said to be the most effective way. When there are constraints for internet users to increase the inbound and outbound bandwidth of their data centers, an option is to utilize the bypass service which is located at the upstream network.
- Deploy CDN - CDN can distribute the content of the website to multiple servers, and users access the services from an adjacent CDN, which can not only improve user experience, but also serve as a supplementary method of anti-DDoS.
- Abnormal traffic cleaning - Clean and filter abnormal traffic through anti-DDoS hardware firewall, to ensure that the company's business will not be affected.

The below diagram depicts a general way as how ISP and cloud operators protect the users from DDoS attacks:

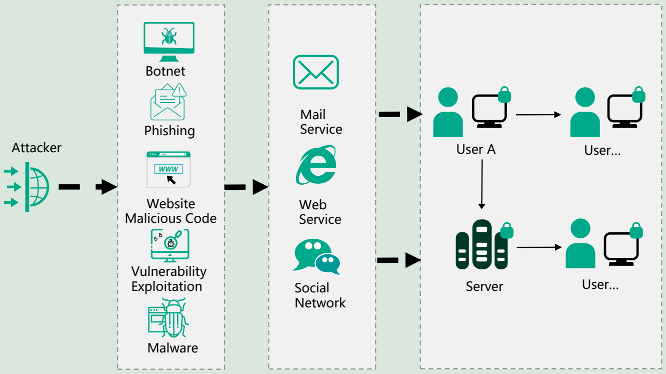
Figure 5. Anti-DDoS process



Threat 2: Ransomware attacks

Ransomware is a member of the Trojan family, which appeared as early as 1989. In recent years, ransomware attacks have occurred frequently.

Ransomware spreads via emails, trojan, and malicious URL injection etc. Once the system is infected, the data is crypted and the victims must pay ransoms to decrypt the data.



Ransomware usually uses a combination of symmetric and asymmetric encryption algorithms to encrypt data. Theoretically it will take hundreds of years to decrypt if using brute force. Therefore, it is usually impossible to decrypt it without knowing the keys.

A Chinese security authority researched the incidents and summarized the situation and trends as below:

- It has become one of the major cyber threats faced by companies in China.
- The attackers are constantly enriching their attack and extortion methods.
- Major systems vulnerable are - Windows, Linux, macOS and industrial control systems.
- Popular ransomwares include DarkSide, Conti, MacRansom, MacSpy, EKANS, Cring etc.
- Multiple extortion models are being developed: “stealing & encryption,”“stealing & encryption & leaking” etc.
- Ransomware attackers is beginning to adopt methods of Advanced Persistent Threat (or “APT”) to launch attacks.
- The ransomware-as-a-service (or “RaaS”) model is the new trend at scale. Driven by the increasing profit, RaaS has been credited as one of the key reasons for the rapid spread of ransomware attacks.
- Ransomware attackers begin to cooperate with the data leakage platforms for added benefits.

Below are the major counter measures adopted in China:

- Exploit operational backup/restore services for important data to minimize the risk of data loss

- Perform system updates and patch management to remove the vulnerabilities
- Use endpoint protection - Install and keep updating anti virus or EDR (Endpoint Detection and Response), shut down unnecessary services and ports
- Use application whitelisting and control
- Improve employee security awareness. For example, require the employees to set stronger passwords, and do not click on links from unknown sources.
- Develop emergency response plans

Threat 3: Data leakage

These are frequent data leakage scenarios:

- Cyber-attacks - Attackers exploit vulnerabilities to break into the target systems to obtain the data
- Insider attack - Internal personnels misuse the privilege and leak the data either intentionally or unintentionally
- Third party leakage - The organization's third-party suppliers continue to use the data after the valid terms of usage. This can either be on purpose or because of improper operations.
- Physical security issues. Examples include loss or theft of unencrypted removable storage devices, or unprotected data backups

According to the "2021 Data Leakage Situation Analysis Report", China's data leakage situation presents the following trends:

- In 2021, the proportion of data leakage accounts for 80% of all data security incidents. Most of data leakage is profit driven.
- Statistics show that among the causes of data leakage, insiders and attackers account for the same proportion, where insiders account for 42% and attackers for 39%
- Among all data leakage incidents, the proportion of personal information leakage is more than 60%, ranking first
- Among the industries where personal information is leaked, internet companies are accounted for the highest proportion, followed by the medical and financial insurance industries, adding up to 60% in total

Meanwhile, the frequency and cost of data breaches have grown rapidly in the recent years. According to the "2022 Cost of Data Breach Report" released by Ponemon, the average cost of global data breaches in 2022 hit record highs.

So how should enterprises deal with data leakage incidents?

Infosys recommends that enterprises establish comprehensive Data Security Governance.

Data Security Governance requires collaboration across entire enterprise. It includes establishing specific teams, formulating data security specifications, building data security technical capabilities, and improving data security awareness. Data Security Governance is focused on the data life cycle, and to build data security capabilities from three aspects, which are Security Management, Security Technology, And Security Operation.

1. Security Management

- Organization buildup - It includes the establishment of teams, RACI matrix, and collaboration mechanisms. It is recommended to assign responsibilities from top to bottom.
- Process & Specification - It is recommended to create different levels of documents including level 1, level 2, level 3, and level 4, to guide the buildup of the data security capabilities on all levels.

- Training & Assessment - Strengthen the awareness and professional competence of personnel performing data security work.

2. Security Technology

It is recommended to adopt NIST CSF IPDRR methodology to build technical data security through the entire data life cycle including different stages of data collection, transmission, storage, in-use, exchange, and disposal. NIST CSF IPDRR methodology could involve the below phases:

- Identify - It's the foundation of the entire framework and can help improve organization's understanding on the risk of systems & data, using technologies such as data management, risk assessment etc.
- Protect - It can prevent the potential data leakage threats, using technologies such as IAM, DLP etc.
- Detect - Data security events can be discovered in time, using technologies such as log audit, continuous monitoring etc.
- Respond - It could contain the impact of incidents, using technologies such as response, mitigation etc.
- Recover - Normal operations can be resumed in time to mitigate the impact of incident, using technologies such as data recovery, improvement etc.

3. Security Operation

The core value of the data security operation lies in discovering, verifying, analyzing, responding, and solving data leakage problems, continuously optimizing the ability to handle security incidents. For the enterprise security, the professional operation is more important than the leveraged products and tools.

Conclusion

Using an EA approach, enterprises can better design the right security capabilities. Some recommendations are given to conform to the minimal set of regulations, and the countermeasures against most seen threats.

In China, compliance is the main driver of enterprise security. With the promulgation of the Cybersecurity Law, Data Security Law and Personal Information Protection Law, enterprises, as compliance entities, need to build related solutions.

Meanwhile, attackers target at high-value businesses which brings data breaches, business continuity risks, and money losses. Among the attacks, DDoS, ransomware, and data breaches are the three prioritized ones.

Authors

Samxuan Wang

Head of Strategy Technology Group, Infosys China

Samxuan is responsible for optimizing architecture capabilities at the architecture, solution, and technology level. He is part of a team that focuses on cybersecurity, infrastructure, cloud migration, data analytics, and the business application of cutting-edge technologies such as machine learning, Web3, and blockchain.

Leo Zhao

Senior Solution Architect of Infosys

He is responsible for cybersecurity service of Infosys in China, focusing on cybersecurity areas such as enterprise security, cloud security and security operations. He has been in the role of a technology architect and solution director in international ICT companies and domestic security companies. He has participated in the formulation of national and industrial security standards. Ning Zhao obtained various cyber security certifications through his related works: CISSP, CISP, DPO, ISO27001

Reference:

1. https://pubs.opengroup.org/architecture/togaf9-doc/arch/

For more information, contact askus@infosys.com

Infosys®
Navigate your next