Protecting Digital Enterprises Against the Rising Threat of Cyber Attacks

S. Sindhu, Research Analyst, Centivens Institute of Innovative Research, Coimbatore, Tamil Nadu, India.
sindhuanbuselvaneniya@gmail.com

Introduction

Digitalization has revolutionized how businesses function, interact, and add value. Cloud computing, telecommuting, interlinked supply chains, and data-driven decision-making are now part and parcel of doing business today. However, just as digitalization has enabled enterprises, so too has it opened up a very wide attack surface to the bad guys – cyber-criminals, hacktivists, and even some state-backed organizations. The more digital enterprises become, the more open they are to attacks, and the number, complexity, and cost of attacks keep increasing each year. This paper discusses the changing cyber-attack landscape faced by digital enterprises and the threats they must guard against.

The Changing Face of the Threat Landscape

A decade ago, cyberattacks were characterized by opportunism, involving mass phishing attacks or general malware circulated in hopes of targeting unsuspecting victims. Today's environment is very different from that of ten years ago in terms of how attacks are carried out.

Ransomware-as-a-Service (RaaS) has led cybercriminals to industrialize their criminal activity, enabling technically unsophisticated people to carry out complex attacks via ransomware by purchasing access to software toolkits created by criminal developers. There has been an explosion in the number of ransomware attacks on organizations of all sizes.

Supply chain attacks- supply chain attacks have become one of the most significant risks facing digital businesses. Using a vulnerable software vendor, managed services provider, or open-source component means that hackers can access numerous other companies via one entry point. Such an attack is especially threatening because it uses the trust companies put into their suppliers.

Business email compromise (BEC) continues to cause considerable financial losses for organizations worldwide. In these attacks, the perpetrators make use of social engineering

techniques rather than taking a technological route by impersonating executives or any other authorized personnel to defraud their targets.

Advanced persistent threats (APTs)- which are typically associated with nation-states, present a totally new type of risk, involving slow and sneaky infiltration for purposes such as stealing intellectual property, spying, or sabotage.

Cloud-native attacks have developed with the growth of cloud adoption by enterprises, making use of misconfigured storage buckets, overly permissive identity roles, and unsecured APIs to gain access to sensitive information stored in the cloud.

Why Digital Enterprises Are Increasingly Targeted

There are various structural reasons as to why digital enterprises have been such tempting targets for cyberattacks in recent times. The first reason is the amount of valuable data – including customers' data, financial data, intellectual property, among other types – that contemporary organizations accumulate and retain, which makes them targets of opportunity for theft and extortion. Secondly, the very fact that businesses have moved towards digitization implies that any compromised system could give an intruder access to many more systems than one; hence, making such attacks quite devastating. The last factor to be considered is remote work.

In addition, the monetization of cybercrime has increased the profitability of attacks and decreased their risks for perpetrators. Payments via cryptocurrency, anonymous infrastructure, and legal jurisdictional arbitrage, by conducting attacks from areas where law enforcement collaboration is low, have provided low barriers to entry for criminals and decreased their chances of being prosecuted.

Core Pillars of Enterprise Cyber Defense

Securing the digital enterprise from such a dynamic threat landscape necessitates a holistic approach to security. The following pillars serve as the basis for enterprise cyber defense.

1. Asset Visibility and Attack Surface Management

To defend a digital business entity against such a dynamically changing threat landscape requires a multi-layered cybersecurity strategy. Below is a list of components that form an enterprise cyber defense strategy.

2. Zero Trust Architecture

The concept of the secure internal network with a fortified perimeter in the context of the cloud, work from anywhere, and third-party access is obsolete. The philosophy of zero trust is "never trust, always verify" whereby each user and each device requesting access to enterprise systems needs to be verified

constantly. This greatly decreases the chances of lateral movement of the attacker once access to the system is gained.

3. Identity as the New Perimeter

Identity has thus emerged as the key point of control for enterprise security, as the network boundaries have broken down in the conventional sense. Robust processes related to Identity & Access Management, such as multi-factor authentication, single sign-on, conditional access, and privileged access management, are vital to prevent any unauthenticated access, considering credential theft and phishing attacks.

4. Endpoint and Network Detection

Since there is no way to know for sure that an attack cannot get through preventive measures, organizations require adequate detection mechanisms. EDR and XDR solutions allow organizations to detect any malicious activity that happens at the endpoint level, network, or cloud.

5. Data Protection and Encryption

Protection of enterprise data during the processes of being at rest, in transit, or in use is key. These measures would include correct implementation of encryption techniques, data classification for protection of sensitive data, and data loss prevention measures for ensuring that there is no unauthorized transfer of data.

6. Resilient Backup and Recovery

Given the prevalence of ransomware, enterprises must maintain immutable, regularly tested backups that are isolated from the production network. The ability to restore critical systems quickly, without paying a ransom, is one of the most effective defenses against the financial and operational impact of a ransomware attack.

7. Third-Party and Supply Chain Risk Management

Due to supply chain attacks, organizations need to take their risk management processes to include their partners, vendors, and software providers. Organizations should conduct security assessments for important vendors, have security requirements in contracts, and watch for weaknesses in the third-party components used in the organization.

Incident Response Readiness

Even for the most secure organization, absolute prevention cannot be achieved. An effective incident response plan is thus an essential part of organizational security. Such a plan will need to delineate clear roles and responsibilities, communications procedures (both within and outside the organization, as well as reporting requirements), containment and mitigation steps, and processes for conducting after action reviews to learn from experience.

Table top exercises are one way of ensuring that the organization has such an incident response capability in place.

The Strategic Imperative

Securing a digital business from the increasing cyber-attacks is not only a technological problem but also a strategic necessity that affects all areas of the business. Businesses that adopt a strategy where cybersecurity is integral to their digital business strategy will be in a position to innovate with confidence and sustain their competitive advantage. This is a continuous process of investments and commitment from the top management as well as making adjustments to security systems in accordance with changing modes of attacks. Organizations that view the expenditure on cybersecurity merely as an expense and not as an opportunity for secure growth in the digital world will find themselves inadequately prepared in a world where the attacker faces no such limitations.

Conclusion

The growing risks of cyber threats to digital businesses have not yet reached its peak. With the growing complexity, coordination, and funding of the cyberattacks, it is imperative that digital businesses counter them with their sophistication, completeness, and agility. Through achieving visibility of their digital resources, adopting a zero-trust approach, improving their identity management, securing their detection and response capability, protecting their critical information, and incident preparedness, digital businesses would reduce their risk profile and increase their resilience in the increasingly contested digital environment.