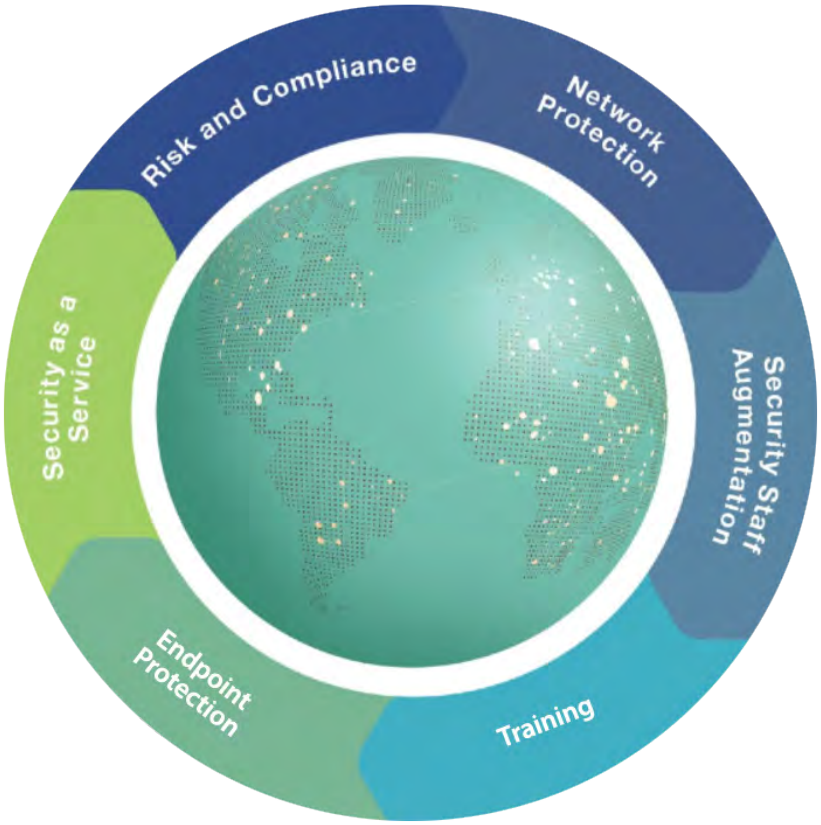
ZCorum™

12 Essential Tips to Protect Your Company from Cyber Attacks

Introduction

There is no escaping the digital world's threats. But you can ensure your company's protection against cyberattacks. This eBook will provide you with twelve essential tips to safeguard your organization's sensitive data and infrastructure. By implementing these measures, you can significantly reduce the risk of falling victim to cyber threats.



1 Employee Education

Educating your employees about cybersecurity is crucial for building a strong defense against cyberattacks. Plan and provide security training regularly on the latest cyber threats and techniques used by attackers. Comprehensive sessions that cover various topics, such as identifying phishing emails, recognizing social engineering tactics, and understanding malware risks will raise staff awareness of how easy it is for attackers to get in. Teach them to create strong passwords, avoid suspicious links, and report any potential security incidents. Encourage them to exercise caution while browsing the internet, downloading attachments, or clicking on links from unfamiliar sources. You can also update your employees on the latest cyber threats and techniques used by attackers through newsletters or internal communication channels.

2 Regular Software Updates

Outdated software including operating systems, applications, and antivirus protection is often targeted by cybercriminals, so staying up to date significantly reduces the risk of exploitation. Regular updates will patch the vulnerabilities that attackers exploit. To avoid missing an update on critical software, enable automatic updates for operating systems, antivirus software, web browsers, and other applications. Implement a centralized patch management system to ensure consistent and timely updates across all devices. Regularly monitor vendor websites, security bulletins, and mailing lists to stay informed about software vulnerabilities and apply patches promptly.

Also, rather than standard antivirus protection on employee devices, consider deploying an advanced endpoint security solution. Endpoint Detection and Response (EDR) protects against file-less and script-based threats by actively scanning all your devices for anomalies and suspicious behavior.

3 Strong Passwords

Strong passwords are a fundamental aspect of protecting user accounts and sensitive data. Enforce a policy of using strong passwords that are unique and complex. Emphasize the importance of using a combination of upper and lowercase letters, numbers, and special characters. Discourage the reuse of passwords across multiple accounts and the use of easily guessable passwords, such as common words, birthdates, or sequential patterns.

Consider implementing a password policy that enforces minimum length requirements and regular password changes. The use of password management tools to store passwords reduces the likelihood of password reuse across multiple accounts which puts multiple systems at risk should a password breach happen.

4 Multi-Factor Authentication

Implementing MFA adds an extra layer of security by requiring users to provide multiple forms of identification beyond passwords to access sensitive systems or data. This typically involves combining something the user knows, such as a password, with something they have, like a unique code sent to their mobile device. This adds an extra hurdle for attackers trying to gain unauthorized access to sensitive systems or data. MFA significantly enhances the security of user accounts by mitigating the risks associated with password-related vulnerabilities, such as weak passwords or password reuse. Implement MFA for critical systems, remote access, and privileged accounts to reduce the likelihood of unauthorized access even if passwords are compromised.

5 Dark Web Research

The dark web refers to a part of the internet that is not easily accessible through traditional search engines. It is often associated with illegal activities and provides a platform for anonymous communication and transactions. Company passwords and accounts are often stolen and offered for sale on the dark web.

Some cybersecurity firms offer dark web monitoring services. These services involve scanning the dark web for mentions of your company's data or accounts, allowing you to be alerted if any compromises are detected. Cybersecurity experts who specialize in incident response and digital forensics can help identify the extent of a data breach, assess the potential risks, and provide guidance on remediation measures.

If you suspect that your company's passwords or accounts have been compromised and are being sold on the dark web, report the incident to your local law enforcement agency or a cybercrime unit. They have the expertise and resources to investigate such matters and can guide you on the appropriate course of action. Conduct regular cybersecurity awareness training to educate employees about the risks associated with the dark web. Encourage them to be vigilant, avoid using personal credentials for work-related accounts, and to report any suspicious activities.

6 Firewall Protection

Firewalls function as barriers between your internal network and the external world, monitoring and controlling incoming and outgoing network traffic, filtering out potentially malicious data packets and preventing unauthorized access. Firewalls rules can restrict access to specific ports and services, and regular updating the rules can reflect changing network security needs. Additionally, implementing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) as additional layers of protection can detect and block suspicious network traffic or attacks in real-time, providing proactive defense against cyber threats.

7 Data Encryption

Data encryption plays a critical role in safeguarding sensitive information, both when it's being transmitted over the internet and stored on devices or servers. Encryption converts data into unreadable form, making it useless to unauthorized individuals who may gain access, ensuring that even if attackers gain unauthorized access, the data remains secure. Encrypting sensitive data adds another layer of protection. Using secure encryption protocols, such as Transport Layer Security (TLS) for internet communication, strong encryption algorithms for data storage and full-disk encryption on devices ensures that data remains secure.

8 Regular Data Backups

Frequent and secure data backups are crucial for mitigating the impact of cyberattacks and ensuring business continuity. This will help recover data in case of a successful cyberattack. Establish a comprehensive backup strategy that includes regular backups of critical systems, databases, and important data. The frequency of your backups is based on the criticality of the data and the potential impact of its loss. Then store your backups offline, in the cloud or offsite to protect against ransomware attacks. Test the restoration process periodically to ensure data integrity and the ability to recover data effectively in the event of a cyber attack or data loss incident.

9 Network Segmentation

Network segmentation involves dividing your network infrastructure into separate segments, each with its own security controls and limited access permissions. This practice reduces the potential damage that an attacker can cause if they gain access to only a single segment of your network. This prevents attackers from moving laterally across the network, containing the damage to a specific segment. You can implement segmentation based on logical or physical boundaries, such as departments, projects, or user roles. Applying access controls and firewall rules to restrict communication between segments allows only necessary traffic to flow. Network segmentation also helps in detecting abnormal network activity, as traffic patterns within each segment are more manageable and predictable.

10 Security Assessment and Incident Response Plan

Developing an incident response plan (IRP) is crucial for efficiently and effectively responding to cyberattacks or security incidents. The IRP outlines the steps to be taken in the event of a security incident, including detection, containment, eradication, and recovery.

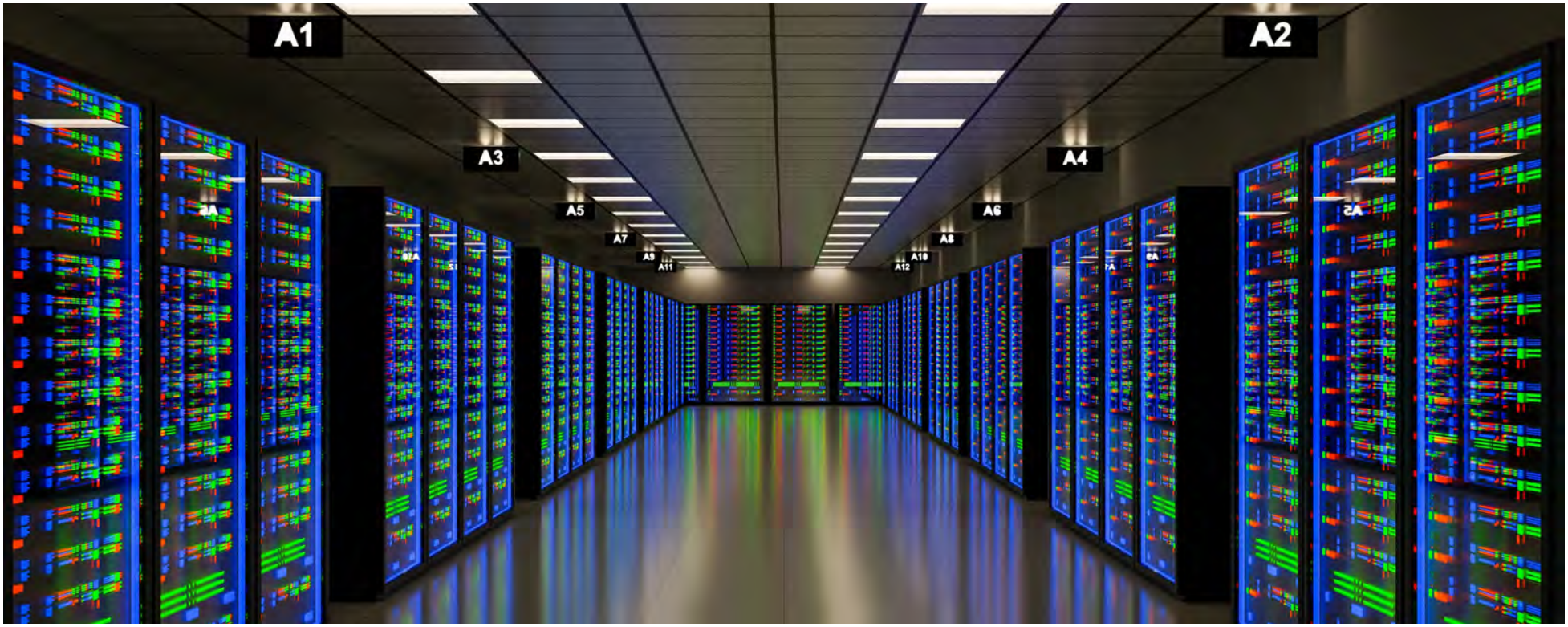
The IRP defines roles and responsibilities of key personnel involved in incident response, including IT staff, security personnel, and management. Communication channels and contact information for reporting incidents and escalating critical issues should be outlined in the IRP.

Regular reviews and updates to the plan should reflect changes in your organization's infrastructure, technology landscape, or emerging threats. You can test and validate the IRP with your staff using tabletop exercises or simulated scenarios to identify any gaps or areas for improvement.

11

Security Awareness Training

Security awareness training is essential for fostering a culture of cybersecurity within your organization. Regularly conduct security awareness training to educate employees about emerging threats, attack techniques, and cybersecurity best practices. Provide practical examples of phishing emails, social engineering tactics, and other common attack vectors like suspicious websites. Encourage employees to report suspicious activities and maintain an open line of communication for security-related concerns. Reinforce the importance of adhering to security policies and procedures, such as data classification, access controls, and incident reporting. Encourage employees to maintain good cyber hygiene, by locking their devices when not in use.



12 Intrusion Detection Software and the SOC

The need for robust intrusion detection software and a dedicated Security Operations Center (SOC) cannot be overstated. With the increasing frequency and sophistication of cyberattacks, providers face significant risks to their network and overall security. Intrusion detection software plays a crucial role in monitoring network traffic, analyzing patterns, and identifying security breaches or suspicious activities. By actively scanning for anomalies and known attack signatures, this software helps detect and respond to threats quickly, minimizing the damage caused by malicious actions.

However, managing and maintaining an intrusion detection system requires specialized knowledge and a round-the-clock vigilance. This is where a SOC staffed with skilled security professionals becomes invaluable. SOC teams actively monitor and analyze the data generated by the intrusion detection software ensuring that alerts are immediately investigated, and actions are taken to mitigate damage. The SOC staff handle incident response, conduct thorough investigations, implement security protocols, and coordinate with other teams to prevent further intrusion. Read how ZCorum can do this for you below.

Next Steps

Cybersecurity is an ongoing process and requires constant monitoring for new threats. Protecting your network is an investment in its long-term stability and reputation. By prioritizing cybersecurity and implementing these twelve best practices, you can significantly enhance your company's resilience against cyber-attacks.

Fortunately, you don't need to do all of this on your own. Let ZCorum be your cybersecurity team. In addition to expert advice on the security policies you should have in place, we offer a managed, comprehensive Cybersecurity Solution that includes intrusion detection software and a fully staffed Security Operations Center that watches over your network 24x7. We can also deploy managed Endpoint Detection and Response (EDR) to protect the endpoints on your network. You can have immediate peace of mind knowing there is a robust defense in place protecting your network and your business from the inevitable threats and attacks that will come. For more information on how we can help, be sure to **visit our website** or contact us at 800-909-9441.

ZCorum™

4501 North Point Parkway,
Suite 125
Alpharetta, GA 30022

ZCorum provides broadband Internet and communication solutions to telcos, cable companies, utilities, and municipalities, assisting in all facets of broadband implementation, integration, engineering and consulting, network monitoring and diagnostics. ZCorum also offers wholesale, privatelabeled Internet services, including data and VoIP provisioning, email, Web hosting, and 24x7 support for end-users, enabling service providers to compete effectively in their local rural and suburban markets. ZCorum is headquartered in Alpharetta, GA.