RANSOMWARE PROTECTION CHECKLIST

Ransomware attackers are increasingly employing more sophisticated attacks and defeating existing defenses. Use this checklist to develop an effective protection plan for your organization.

1. Protect your email.



Ransomware attacks often start with a phishing email to capture admin or user credentials.

1a	**Block phishing attacks** Attackers use social engineering tactics to bypass traditional email security. Use an email security solution that includes AI-enabled phishing and account takeover protection, as well as alerts when malicious activities are detected.	☐
1b	**Train users** Your users are your last line of defense against phishing attacks. Training needs to be an ongoing effort, as attacks often become more sophisticated over time.	☐
1c	**Implement remediation** Email attacks that evade email security and land in users' inboxes need to be addressed quickly. Choose an email security solution that enables proactive threat discovery and automates remediation.	☐

2. Secure your applications.



Attackers hack your web applications to gain access to your data.

2a	**Protect web applications** Applications often have open vulnerabilities that can be exploited to gain access to your data. Use an application security solution that defends against web application vulnerabilities such as OWASP Top 10, zero-day and brute force attacks.	☐
2b	**Protect access to applications** For internal applications, you should only allow access for authorized users and devices. Choose a zero trust access solution that enables role based access, multi-factor authentication and continuous verification of user and device identity.	☐
2c	**Prevent lateral movement on your network** If attackers gain access to your network, they often attempt to move laterally to find and infect data sources. You need a network firewall that protects both your on-prem and cloud networks with network segmentation and advanced security services.	☐

3. Back up your data.

Attackers encrypt your data and demand ransom.

3a	**Back up your data** You need to back up all of your data. Remember your on-prem data as well as data in the cloud/SaaS applications such as Office 365.	☐
3b	**Protect access to applications** Attackers often target your backups to prevent you from being able to recover your data. Encryption, access control, and IP restrictions are all important here. You want to make sure that accessing your data is easy for you, but difficult for attackers.	☐
3c	**Develop a recovery plan** If you are under attack, you need to be able to quickly deal with the attack, recover your data and avoid paying ransom. Consider not only your technical response, but also your business response. Test your plan in full before there is a problem. Forensics can be helpful in the aftermath of an attack to find vulnerabilities.	☐

Other Recommendations

• **Patching** – Make sure software is patched and up to date. Attackers look for known vulnerabilities first, so don't make it easy for them.
• **Password Security** – Enforce strong passwords. Many recent attacks were successful due to weak passwords and ineffective password management practices.
• **Multifactor Authentication** – Consider requiring a phone app or text based second factor authentication for all applications and resources. This is very useful in preventing brute-force login attempts.

Build your ransomware plan.
https://www.barracuda.com/ransomware

Reach out to K Group Companies for help implementing this checklist:
https://www.kgroupcompanies.com/contact

Barracuda
Your journey, secured.

GROUP
COMPANIES est. 1980

(888) 235-6860
info@kgroupcompanies.com
www.kgroupcompanies.com

678 Front Ave NW, Suite 003
Grand Rapids, MI 49504

• US 1.0 • Copyright 2020 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com
Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States. All other names are the property of their respective owners.