Recovery Security Checklist

Change Passwords

- [ ] If Active Directory (AD) was compromised, this includes if a suspected a Domain Controller sync (DC sync) was conducted by the adversaries, then all AD accounts need to have their passwords changed before the AD is brought online for service to the network.

- [ ] Local Passwords of all compromised system need to be changed. If the same Local Password is used across all devices, consider implementing Local Administrator Password Solution (LAPS) in the future.

- [ ] The authentication to all devices, services and vendor sites that where compromised need to have the passwords changed. This includes the online and Cloud based services, SaaS platforms for your business.

- [ ] Including all services that a browser profiles automatically stored credentials for.

Enable Multi-Factor Authentication (MFA)

- [ ] If MFA has not yet been enabled on authentication credentials that were compromised, enable MFA on them now.

- [ ] We recommend implementing an MFA policy to enforce the use of MFA on user accounts for the domain, but also for 3rd party services

Rotate API Keys, Key Pairs and Encryption Keys

- [ ] Compromised API keys or servers or application/services the API keys are generated on or are stored on need to be rotated.

- [ ] Security key pairs used for secured logins (ie. RSA Keys) for services such as SSH, SFTP need be rebuilt and changed for all users who's private keys where compromised.

- [ ] All encryption keys that where compromised need to be rotated. This includes encryption keys used for backups, applications, or other services.

Updates

- [ ] Operating Systems need to be updated. This includes Windows Updates, Linux updates or Hypervisor Updates.

- [ ] Software on every device should be updated to the latest version. There may be some scenarios where certain software cannot be updated but might have a security patch available. We recommend all security patches that are available are installed prior to going production.

- [ ] For outdated software that no longer provides updates, we recommend looking into updating these systems to something more modern after the restoration process is complete.

AV & EDR

- [ ] Ensure anti-virus is running on every device. Windows Defender is a great start anti-virus software, but Windows provides more in-depth anti-virus solutions.

- [ ] We recommend using an EDR solution like Carbon Black or MalwareBytes Endpoint Detection and Response for businesses if you don't have an EDR solution. EDR solution(s) should have cloud-based logging and monitoring, to retain activity logs. It should also provide the capability to block applications from running, and this should be tuned properly for your business to reduce the attack surface. Ensure the agent is installed and configured prior to moving to production.

Backups

- [ ] Ensure the Backup Agent is properly installed and functioning on every device prior to moving to production.

Improvements

Hardening Controls and Network Protocol security should be considered after the business is recovered and operational.

Firewall

1. Review firewall policies for your networks and devices, ensure a proper audit is conducted and that the potential attack surface that can be minimized, are corrected. This can include access control lists (ACL) that provide too much access, the port range could be too great, or the accepted IP range is too large.
2. Find network protocols that are insecurely configured or lacking authentication/authorization. Especially protocols like OSPF, or even service protocols like SNMP versions that don't use authorization, these should be reviewed, and a plan conducted to migrate these protocols and services to a more secure configuration.

As it could be significant work, it's recommended to focus on getting the business operational before prioritizing the sizeable changes. However, simpler changes like ACLs should be addressed immediately.

Hardening Controls

1. Frameworks such as CIS or NIST can provide security hardening controls for operating systems and services. We recommend looking into these hardening frameworks as a security baseline for your business. These should be considered after the business is operational.
2. Group Policy Objects (GPO) can be leveraged to implement additional security controls across an entire domain. We would recommend obtaining professional advice on upgrading your GPOs to tighten up your environment moving forward.