LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

LOGmanager - Best Practice to minimize Ransomware threat

Long story short: Today, as everyday, a lot of malware is being created, utilized and at the end of the day - also monetized. One of the most popular and "successful" types of malware in current threat landscape is Ransomware. It spreads easily, while damage it does is substantial. To minimize damage, that can be caused by adversaries, LOGmanager security team suggest a set of best practices and countermeasures to follow. We do not claim that this is a complete set of rules and policies to apply, but it provides a strong foundation. If Your company IT will consider at least some of them, it will certainly create a pretty hardened playground for bad actors to accomplish their destructive mission.

Network infrastructure best practices

1.	Implement Firewall rules not only for inbound, but carefully limit the outbound rules. Best practice would be also to implement a kind of whitelist for what is allowed to access. Log all the firewall traffic, except deny in the inbound of perimeter zone. Compare zone rules for efficiency by analysing rules hit rate in log management.	☐
Notes:		
2.	Internal network segmentation via Firewall. Implement internal security zones and create rules on least privilege logic to be a limiting inter zone communication. If possible, log also all non-perimeter firewall traffic.	☐
3.	Segmented Virtual LANs (802.1Q) should be deployed, where possible with port-isolation or private-vlan mode. If ACL's deployed in inter-vlan communication (instead of Firewalls), log all permit/deny hits.	☐
4.	Implement Network Access Control based on 802.1X. If the given device connected to network does not allow to use 802.1X supplicant, use fallback to MAC based authentication. Log both authenticator (LAN, WLAN) and authentication server events. Do not permit domain computers connect to guest VLAN and use of domain credentials to 802.1X auth.	☐
5.	Implement Intrusion Prevention rules on at least perimeter internal port of NG Firewall. Apply the security optimized profile and log all the IPS events.	☐
6.	Mandatory "always on" VPN with disabled split tunnels. All the remote workstation traffic should pass through company firewall hence ensuring the defined rules are always applied. Log all the VPN traffic, pay attention to geolocation of incoming VPN connections and excessive outbound traffic (possible traffic exfiltration).	☐
7.	Contact Your network infrastructure partner and review, if best practice for spoofing detection/prevention are applied (ARP inspection, Port security and DHCP Snooping). Log all those events and notify alerts.	☐

MS AD best practices

1.	Divide AD admin roles. Domain admin should connect with this account only to DC servers, if such connect to anything else, consider it compromised and change the password ASAP. Same for the servers. Server admins can use their account only to connect to AD servers, not to anything else including workstations and/or DC. Log all admin activities.	☐
Notes:		
2.	Create special user with delegated rights to add computers into domain. Log adding new users and computers into domain.	☐
3.	Switch to Kerberos only authentication in MS AD environment. First Audit NTLM and Log all the NTLM audit for a week. Then based on audit results – create exceptions and restrict NTLM authentication ("Deny all" is the best approach; "Deny for Domain Servers" – at least) in Group Policies. Reference link.	☐
4.	Disable local admins. None of workstation users should be local admin. Use helpdesk/support accounts only. Helpdesk/support admin should not be server admins. Log and notify any local admin activities.	☐
5.	Consider application whitelisting and overall use of applocker and its capabilities to restrict running executable files from other than program files folders. Log all applocker activities. Reference link1. Reference link2. Reference link3.	☐
6.	Customize and install Administrative Template files for O365 and Office. Limiting all users opening documents with Macros only to documents, where Macro is signed with local certification authority (best practice) or block macros from running in Office files from the Internet (at least). Reference link.	☐
7.	Log all CLI commands run on servers. Notify CLI activity off working hours.	☐
8.	Log all WMI communication and notify all remote WMI tasks during off working hours.	☐
9.	Maintain proper patch management. Log windows update activities and notify failed updates on servers hosting applications, pay attention especially to servers facing Internet/DMZ security zones.	☐
10.	Get rid of older versions of SMB protocol. Periodically review SMB folder access right and log all SMB activities – Advanced Audit Policy – Detailed File Share.	☐

Backup best practices

Only thing that will provide 100% protection from malware unrecoverable disaster is backup! Only if you have properly stored backups (onsite, offsite, offline) you can recover your data back! Periodically verify, that you can restore data from backups.

1.	Backup all important data periodically, review/monitor and alert that backup procedure is working fine. Log all backup server configuration changes and all backup operations. Notify failed backup operations.	☐
Notes:		
2.	Backup server should not be a part of the domain and user/password used on Backup server should be strong and different from any admin account used in AD. Log all access to backup server. Log backup server network activities.	☐
3.	Restrict network access to backup server to permit only TCP/UDP ports, backup server needs to utilize. Log firewall policies restricting access to backup server. Place backup server to special VLAN.	☐

Other best practices

1.	Get rid of all remote desktop applications which allows unrestricted access to company resources (aka teamview). Log use and monitor utilization of permitted remote desktop applications. Notify use of new remote access enabled applications.	☐
Notes:		
2.	Use trusted Antivirus solution with central management. Log all Antivirus activities via its central management, notify on disabled AV engines from all workstation and servers.	☐
3.	Implement IPS with build in SSL proxy for outbound traffic. Log all IPS activities.	☐
4.	Implement Sandbox inspection of inbound files for web and email traffic. Log all sandbox activities and notify those detecting threat.	☐
5.	Log all DNS queries and analyze for DNS covert channel.	☐

Other security enhancements to consider

1.	Via log management, discover use of unsecured protocols and replace them with secured ones. Pay attention especially to Telnet, SNMPv1/v2c where the write access is permitted, FTP and vulnerable SMBv1.	☐
Notes:		
2.	Implement vulnerability scanning.	☐
3.	Log Linux admin activity including command issued in CLI. Notify on atypical or dangerous commands. Sample commands to notify on: *history; cat /home/*/.ssh/id_rsa; python -m SimpleHTTPServer; python -m http.server; nc -e /bin/sh; nc -l -p;… Reference link.	☐
4.	Via log management, monitor all Internal-IP <—> External-DNS-PTR connection pairs and check pairs with excessive amount of connections or overall long connections. Use ASN #/names to exclude trusted external networks from the list.	☐
5.	Log and notify any non NTP driven change of time/date and stop logging (stop syslog) operations.	☐
6.	Educate users on password policies. (Mention specifically the mandatory ban on using company email to register private accounts and need to use different passwords for any use on internet)	☐

Conclusion: Having all of these practices in place will definitely help in securing your environment. But as threats evolve, so should your defences. Security is always an incremental process and it is important to regularly check, if your system is in good shape and can defend against latest attack vectors. Every time you add new software or hardware, or make other major changes to your infrastructure, address how you will include these changes in your security policies and audit them in your log management. And the most important advice - plan and be prepared for unexpected, especially in the response to eventual security incident.

Please, provide feedback and suggestions on this whitepaper to security-team@logmanager.com.

ABOUT THE MANUFACTURER

LOGmanager has been developed since 2014 as a flagship product of Sirwisa a.s., a company based in Prague. You can find selected customer references at www.logmanager.com. Our customers include not only government authorities, but also businesses of all sizes from all sectors, business corporations, banking organizations and more. Do not hesitate to contact us for more detailed customer references directly from your area of business. We will be happy to provide contacts to existing customers, who have agreed to be included on our list of references.