How PAM Helps to Protect Your Business from Ransomware Attacks

The art of defense

Since existing defense solutions often fail to detect ransomware or prevent it from infecting and spreading within the network, businesses are facing severe risk of high ransom fees and data loss. However, all is not lost since there are many actions one can take in order to mitigate the risk of ransomware:

- Regular backups: a business that often backup their data can avoid paying the ransom since the cost of potential data loss will be minimal.
- Regular updates: most ransomware use existing vulnerabilities and businesses with up-to-date systems have a much lower risk of being infected.
- Constant activity monitoring: monitoring all network activities enables security teams to identify and prevent potential malicious activities before they are able to cause any damage.
- Employee education: ransomware such as Locky which we mentioned above, uses spam and phishing methods to infiltrate the network and educating employees on security best practices further mitigates risk.

Last but not least, enforcing endpoint security by combining privilege access management and application control, gives businesses an effective way of mitigating risk of ransomware. By doing this, businesses can easily remove local administrator rights which some ransomware require, as well as to control applications, thus preventing unknown applications from executing.

With **Privileged Account Management**, businesses can do exactly the above – combine privilege account management and application control. By controlling local admin privileges, business significantly reduces the attack surface as it allows trusted applications to run while preventing ransomware that requires admin rights from executing. Besides focusing on protecting the outside network parameter, PAM adds several protection layers on the inside by protecting admin credentials, controlling privileged user's access and monitoring their activity across all IT resources. PAM is an easy-to-deploy solution that is able to protect your complete network infrastructure: from traditional physical data centers to virtual and cloud platforms such as AWS and Rackspace. Each attempt of misuses automatically revokes access privileges and sends out alerts to your cyber security teams.