CyberArk Secures Primary Targets in Critical Infrastructure Attacks â€“ Privileged Accounts

November 7, 2012 4:01 PM ET

Privileged Identity Management Suite for Critical Infrastructure Protection Secures and Manages Privileged Access in SCADA, ICS, Smart Grids and other Operational Technologies

NEWTON, Mass. - November 27, 2012 - Cyber-ArkÂ® Software today announced the release of its Privileged Identity Management Suite for Critical Infrastructure Protection (PIM/CIP) to secure, manage and monitor all privileged account access and activities across Operational Technology (OT). The solution secures critical infrastructure by preventing the exploitation of local or remote access to privileged accounts â€“ the primary target of Industrial Control Systems (ICS) and SCADA cyber-attacks.

Privileged Accounts Emerge as Primary Target of Critical Infrastructure Attacks

- Organizations that serve as national critical infrastructure have interconnected corporate IT systems with production and OT environments that were traditionally segregated. Connecting ICS, SCADA and other OT systems to corporate networks has introduced known risks from the IT environment into the OT environment â€“ including the exposure of privileged access points.
- Privileged access points consist of privileged and administrative accounts, default and hardcoded passwords, application backdoors, and more. These accounts act as a gateway to an organization's most sensitive production systems, which control the production and delivery of electricity, water, gas and other critical services to the public.
- The typical operational environment consists of thousands of servers, databases, SCADA RTUs and PLCs, network devices and applications â€“ all controlled and managed by a variety of privileged and shared administrative accounts. Built-in vulnerabilities, including hardcoded and factory default passwords, are also known problems in OT and SCADA systems. The security, control and auditability of these privileged access points are often neglected, while usage is hard to monitor.
- A recent alert 1 from The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) highlighted that the combination of network connectivity with these known vulnerabilities would "significantly increase the ICS threat landscape."
- The report further stated that critical infrastructure companies should "not assume that their control systems are secure or that they are not operating with an Internet accessible configuration. Instead, asset owners should thoroughly audit their networks for Internet facing devices, weak authentication methods, and component vulnerabilities."

PIM/CIP Secures Critical Infrastructure â€“Protects the Privileged Pathway
Cyber-Ark's PIM/CIP identifies, secures, manages and tracks all privileged account access and activities across the operational environment, preventing potential cyber-attacks by controlling and monitoring all privileged activities. Cyber-Ark PIM/CIP enables critical infrastructure organizations to:

- Minimize Insider Threats and External Cyber-Threats â€“ Privileged credentials have emerged as the primary target for cyber-attackers â€“ including internal and external attackers. PIM/CIP identifies all privileged accounts across critical infrastructure and secures the use of these shared accounts by identifying users with authorization, providing full accountability and account usage (audit trails).
- Manage Privileged Identities â€“ Organizations can manage privileged passwords and control access for the thousands of remote devices that connect to a network. PIM/CIP enforces policies and workflows around privileged password usage, strength and automatic replacement.
- Secure and Monitor Remote Vendor/Contractor Access â€“ Enables external contractors to have a secured and

transparent connection into the network while isolating the critical network from the threats of malware -- all without divulging system passwords. PIM/CIP provides complete real-time monitoring and recording capabilities of all privileged sessions for forensic analysis and change management review. Organizations are able to terminate suspicious activity in real-time.

- Achieve Compliance with NERC CIP Standards â€“ Cyber-Ark PIM/CIP automates controls to meet NERC CIP regulatory requirements and continuous audit readiness. Organizations can create audit ready processes and policies for password strength, periodic password replacement and role-based access control.
- Reduce Operational Costs â€“ A flexible policy management engine discovers, provisions, automates and replaces hundreds of thousands of privileged credentials across the ICS network and the Smart Grid, eliminating resource-intense manual procedures. This minimizes energy fraud/theft in smart meters by restricting access and creating accountability.

"The built-in flaws of ICS and OT systems have left our critical infrastructure increasingly vulnerable to attacks. As we saw with Stuxnet, the Shamoon virus at Saudi Aramco, and similar high-profile attacks, privileged account vulnerabilities have emerged as the priority target for cyber-attackers," said Roy Adar, vice president of product management, Cyber-Ark Software. "Cyber-Ark's PIM/CIP identifies and protects these privileged access points, securing each organization from the inside out. In addition, the suite provides a comprehensive audit trail for ensuring compliance regulations laid out by NERC CIP, CFATS and NRC."

For more information, visit the website or download the following whitepapers: Cyber-Ark for Critical Infrastructure Protection, Cyber-Ark for Secured Remote Access and Complying with NERC CIP Standards.

About Cyber-Ark

Cyber-ArkÂ® Software is a global information security company that specializes in protecting and managing privileged users, sessions, applications and sensitive information to improve compliance, productivity and protect organizations against insider threats and advanced external threats. With its award-winning Privileged Identity Management, Sensitive Information Management and Privileged Session ManagementSuites, organizations can more effectively manage and govern data center access and activities, whether on-premise, off-premise or in the cloud, while demonstrating returns on security investments. Cyber-Ark works with more than 1,100 customers, including more than 35 percent of the Fortune 100. Headquartered in Newton, Mass., Cyber-Ark has offices and authorized partners in North America, Europe and Asia Pacific. For more information, please visit www.cyberark.com.

1 ICS-ALERT-12-046-01Aâ€“Increasing Threat to Industrial Control Systems, Oct. 25, 2012

Tuesday, November 27, 2012 - 15:00