CONCEPT NOTE - NOVEMBER ISSUE

Issue Theme: Zero Trust, Identity Access Management + Privilege Access management

Today, an organization’s IT assets are dispersed and in hybrid environments. 20 years ago, it was all behind the safe confines of a corporate firewall, with the IT team having complete control of these assets. As employees became mobile and work travel increased, the mobile assets had to be monitored and governed using certain technologies like Mobile Device Management. And then we experienced the BYOD era. First, the senior executives wanted to use their svelte and shiny personal devices at work. And later, other employees wanted to bring their smartphones, tablets, and laptops to work — asking for connectivity.

When the pandemic came along, the workforce became remote overnight, and there was little time to reconfigure the security of employee endpoint devices. Adversaries were well aware of the weak security on employees’ home networks and endpoint devices used in the home. So remote users are increasingly targeted. The threat surface expanded. That led to a jump in ransomware, BEC and other types of attacks on organizations. The unsecured home network (and careless employee behavior) became easy targets for hackers.

Once accounts are compromised, hackers try to escalate their access until they get to privileged accounts, which are the keys to the kingdom (admin access).

The security world responded by enforcing “Zero Trust” policies, security frameworks from NIST and others, identity access management, intrusion detection systems, and privilege access management.

The Zero Trust Model

The Zero Trust model was created in 2010 by John Kindervag, then the principal analyst at Forrester Research Inc. John is also on the CISO MAG Editorial Advisory Board.

But it’s only now that corporates have started implementing Zero Trust, as its supporting technologies move into the mainstream. The pressure to protect enterprise systems and data grows significantly, as attacks become more sophisticated and increase in volume.

So, where are we today? Are we finally doing “information security,” right?

November Issue

The issue will have articles written by experts on Zero Trust and the latest security systems to protect remote workers from cyberattacks. It will provide perspectives, insights, and opinions on the state of enterprise security today. What technologies and frameworks are used today? What should security policies consider?

The editorial team invites articles from experienced subject matter experts. Our editors would like to chat with experts.
To contribute to this issue, please write to:

**The Editor:** brian.p@eccouncil.org (Brian Pereira).

Input deadline: **October 15, 2021**