opentext™

Flash Point Paper

Ransomware: Preventing Hostage Data

Cybercriminals take advantage of a vulnerability in your environment to infest your systems with malware that encrypts your vital business data so it's unusable until you pay them to decrypt it. In some cases, they even steal the data and threaten to release it to your competitors or sell it to the highest bidder.

The WannaCry and NotPetya ransomware attacks have been two of the most devastating incidents in history. WannaCry cost businesses between $4 billion and $8 billion. Losses due to NotPetya were estimated at more than $10 billion. What makes ransomware attacks so dangerously effective is that they are self-propagating. They detect and leverage vulnerabilities in your network and software to gain escalating access to other network devices and data across your environment until the intruder cripples and holds hostage your entire enterprise. As frightening as the prospects of a ransomware attack can be, the reality is that implementing a few simple best practices is typically all that is needed to keep you safe from such attacks.

Prevention Is the Best Defense

Perhaps the biggest irony of most ransomware incidents is that they easily could have been avoided. Ransomware attackers usually exploit well-known vulnerabilities that if victims take known best-practice steps to correct, the attempts to infiltrate their environments will simply fail. Those best practice steps involve keeping all their systems and software patched with all the latest security updates. For example, a month before the WannaCry and NotPetya attacks began to wreak havoc, Microsoft hadfe their02Tw T*heir02Tw sttwract sttuang (anet()0.8.7(emp.02 Tc8.7(f)-2MC Lang ę Tc8.2Lang ę TcP e TcPn-BMC