Malthe Winje

Supportdokument

IT-säkerhet

På senare tid har nätverk runt om i världen utsatts för en IT-attack kallad Petya.
För att skydda sig mot Petya ransomware rekommenderar SBC följande åtgärder för Microsoft Windows-system;

1. Det är viktigt att Windowssystemen är uppdaterade med den senaste mjukvaran och speciellt med Microsoft Security Update 4013389 (http://go1.honeywell.com/o03z700EM00d0R100XJr0X0).

2. På samma sätt som den tidigare storskaliga attacken ("WannaCry") har den här typen, som går under namnen "Petya", "NotPetya", "ExPetr", etc. i pressen, möjlighet att attackara fullt uppdaterade system om så bara en dator i nätverket inte är uppdaterad. Det gör det genom att dumpa referenser från den inte uppdaterade maskinen och använder dem för att attackera de uppdaterade maskinerna i samma nätverk. Så det är väldigt viktigt att alla maskiner på nätet är uppdaterade med den senaste mjukvaran. Och glöm inte virtuella maskiner som kör Windows också.

Det är utan tvekan så att stark cybersäkerhet är ett resultat av gott samarbete mellan tillverkare, systemintegratörer och slutkunder.
System som går att komma åt på distans är inte ovanliga. Vi rekommenderar er att distribuerar systemen på ett säkert sätt bakom en brandvägg eller i ett privat, virtuellt nätverk för att förhindra att obehöriga kommer åt det.

Nedan listar vi några enkla steg som måste följas och vi uppmanar er starkt att följa dessa vid alla aktuella installationer, både kommande och befintliga.

Förhindra obehörig fysiskt tillgång till utrustningen.
Se till att all utrustning har den senaste mjukvaran och FW.
Se till att alla PC har ett virusskydd som är uppdaterade för de senaste virusdefinitionerna.
Se till att all utrustning har inloggning med användarnamn och lösenord/PIN-kod.
Isolera och skydda utrustningen med hjälp av antingen “air gapped networks” eller genom att konfigurera dem i VLAN.
Anslut aldrig utrustningen direkt mot internet.
Om fjärråtkomst krävs – använd VPN.
Se SBC:s allmänna säkerhetsregler för hur ett nätverk ska planeras (26-620) under http://sbc.do/U9jmfkya.

Saia arbetar ständigt för att säkerställa att bästa praxis för cybersäkerhet används under hela utvecklingscykeln för sina produkter.

De berörda produkterna som använder Windows är:
- Saia PG5 och relaterade tilläggsprogram
- Saia Visi.Plus
- SBC OPC Server
- Windowspaneler PCD7.D6xxx
- SBC Micro Browser för Windows