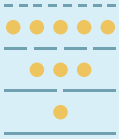
10 åtgärder för SCADA-säkerhet

En sammanställning av olika typer av säkerhetsfunktioner.

1. Skydd mot skadlig kod

Smittade webbplatser och misstänkta e-postlänkar eller e-postbilagor är två vanliga attackvektorer som kan leda till att skadlig kod smyger sig in i ditt system. Det bästa skyddet finner du i antivirus-programvara med funktioner som automatisk uppdatering, borttagning av skadlig programvara, webbläsarsäkerhet och upptäckt av alla typer av smitta.



2. Segmentering

Segmentering innebär att man delar upp systemen i olika säkerhetszoner. Detta kan man göra eftersom alla system inte är lika skyddsvärda och att skydda all information som om den vore det blir varken praktiskt eller ekomiskt försvarbart. Korrekt utförd segmentering resulterar i ett djupförsvar som effektivt kan emotstå även en sofistikerad attackerare.

Processen innebär att alla informationsflöden mellan systemen övervakas och monitoreras, d.v.s. att information kontrolleras innan den får komma in i en zon (för att skydda integriteten i zonen), samt kontrolleras innan den får lämna zonen (för att skydda zonens konfidentialitet).

En säkerhets-/informationspolicy styr vilka som är de tillåtna informationsflödena.

3. Övervakning & loggning

Driftövervakning används för att övervaka verksamhetens IT-system, främst när det gäller tillgängligheten. Ur säkerhetssynpunkt är det viktigast att man övervakar de säkerhetsfunktioner man har installerade.

Loggning innebär att information om händelser i systemen spelas in och lagras med tidpunkt och vilka resurser som var inblandade. Ett loggningssystem kan till exempel övervaka operativsystem, databashanterare och applikationsservrar eller applikationer. Med hjälp av loggningen kan man sedan följa upp på avvikelserna. Att ha intrångsdetektering/skydd, åtkomstkontroll o.s.v. utan att ha loggning med ”incidentrespons” är ungefär som att ha ett tjuvlarm men sedan inte bry sig eller göra något när larmet löser ut.

4. Identitets- och åtkomstkontroll

Olämpliga behörigheter och gamla användarkonton innebär ökad risk för bedrägerier och obehörig åtkomst till känslig information. En väl fungerande hantering av behörigheter leder till att dessa risker minskar, att användarupplevelsen förbättras (kortare ledtider för behörighetsbeställningar) och att kostnaderna reduceras (såsom för licenser, helpdesk och administration).

En viktig åtgärd är att konton ska vara personliga och att det ska finnas få administratörskonton.

Utloggningar ska ske automatiskt så långt det är möjligt (alltid i fallet med administratörskonton).

I SCADA-miljöer är maskinkonton minst lika vanliga som konton knutna till en person. Även denna typ av konton ska vara per maskin eller tjänst.

En annan viktig sak är lösenordshanteringen. Det är t.ex. inte bra ha samma lösenord på olika konton. I vissa fall räcker inte bara lösenord för autentisering utan man måste införa multifaktor-autentisering.

5. Intrångsdetektering

Intrångsdetektering är processen för att identifiera olovlig aktivitet i nätverk och system. Ett intrångs-detekteringssystem analyserar information från olika källor i syfte att identifiera möjliga säkerhets-överträdelser. Glöm inte att övervaka systemen och agera på larmen som genereras (se loggning).

6. Kryptering

Kryptering är att göra information omöjlig att läsa för alla som inte ska kunna läsa den. För att göra informationen läslig igen krävs dekryptering. På så vis skyddas informationen helt mot obehörig avlyssning. Kryptering ska användas när information transporteras över något media eller kommunikationslänk som man inte har fullständig kontroll över. Notera att kryptering kan vara onödigt och kontraproduktivt från ett säkerhetsperspektiv. Exempelvis måste trafik som överförs mellan zoner övervakas och kontrolleras, vilket krypering kan försvåra (se Segmentering).

7. Härdning

Att härda en dator innebär att man säkerställer att endast de användarbehörigheter som behöver finnas på en given dator finns där, övriga tar man helt enkelt bort. Du tar bort eller inaktiverar funktioner i datorn som inte behövs i syfte att minimera antalet potentiella attackvektorer. Du ser också till att systemet uppdateras/patchas. Man tar även bort eller inaktiverar funktioner i datorn som inte behövs för det den ska användas till. Den lokala brandväggen konfigureras till att bara tillåta det nödvändiga. T.ex. blir det gamla och sårbara protokollet SMBv1 fortfarande ofta påslaget vid installation av Windows-baserade system.

8. Mjukvaruuppteringar

De säkerhetsuppdateringar som kommer med jämna mellanrum på en dator eller annan enhet ska man verkligen se till att göra. Då säkerställer man bästa möjliga skydd och tar bort onödiga säkerhetshål.

9. Säker fjärråtkomst

Många organisationer är beroende av fjärråtkomst via RDP, t.ex. för att leverantörer skall kunna utföra underhåll, eller att driftpersonal skall kunna övervaka en anläggning. Fjärråtkomsten innebär att det finns risker för såväl felkonfiguration som implementationsbuggar. Fjärråtkomst kan göras säker genom att använda RDP och skydda jumpservern med en explicit säkerhetslösning.

10. Fysisk säkerhet

IT-säkerhet och fysisk säkerhet går ”hand-i-hand”. Det spelar ingen roll om man skyddar sitt IT-system ”logiskt” med åtkomstkontroll, segmentering, härdning, osv. om man tillåter fri fysisk tillgång till systemen eller direkt till den process som systemen är ämnade att styra.

Vi på Advenica har stor erfarenhet av generella säkerhetsanalyser (risk- och säkerhetsanalyser) liksom säkerhetsskyddsanalyser. Vi kan ge råd om hur du kommer igång med kartläggning av processer och rutiner utifrån ett säkerhetsperspektiv. Vi tillhandahåller också expertis och unika, tekniskt avancerade, hållbara och framtidssäkra cybersäkerhetlösningar med hög assurans för kritisk data-in-motion upp till Top Secret-klassificering. Kontakta oss på advenica.com/sv/kontakta-oss

advenica

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED