ZO BEVEILIG JE EEN INDUSTRIAL CONTROL SYSTEM

Traditionele IT-oplossingen zijn niet veilig genoeg

EEN INDUSTRIAL CONTROL SYSTEM (ICS) BESTAAT UIT TALLOZE KLEINERE SCHAKELS IN EEN KETTING DIE ESSENTIEEL KAN ZIJN VOOR HET VOORTBESTAAN VAN EEN LAND, REGIO OF BEDRIJF. EN DAT TERWIJL HET 'RISICO-OPPERVLAK' VAN EEN ICS GROTER KAN ZIJN DAN BIJ CONVENTIONELE IT-SYSTEMEN, WAARSCHUWT DEAN PARSONS. HOE BEVEILIG JE EEN ICS EN HOE KAN IT ZICH WAPENEN TEGEN ZO'N ALLESOMVATTENDE CYBERSECURITYDREIGING?

door Dean Parsons beeld Shutterstock

ELK SYSTEEM DAT IETS TE MAKEN HEEFT MET HET AANSTUREN VAN IETS IN DE FYSIEKE WERELD IS FEITELIJK EEN CONTROL SYSTEM; in industriële omgevingen zijn die systemen vaak complexer, er is raakvlak met essentiële infrastructuren. Denk hierbij aan het elektriciteitsnet van een land, een waterzuiveringscentrale of een complex voor zware industrie. Stel dat een elektriciteitsnetwerk uitgeschakeld wordt door een cyberaanval of fysieke wapens. Dan zitten ziekenhuizen, waterzuiveringsinstallaties, telecommunicatieproviders en hulpverleners zonder stroom en zijn de gevolgen niet te overzien. Pas als een (ICS) faalt - kijk naar recente aanvallen op essentiële infrastructuren in Oekraïne - wordt het belang van beveiliging echt goed duidelijk.

Daarom moeten cyberbeveiligers binnen de engineeringsector beginnen bij het bepalen van de risicotolerantie en het risico-oppervlak van een algeheel industrial control system en de individuele schakels die dit systeem vormen. Wat zijn de gevolgen van het wegvallen van een onderdeel op de bijbehorende productie, veiligheid en de omgeving en hoe kunnen deze onderdelen worden beveiligd?

Daar ligt een belangrijke realisatie aan ten grondslag, namelijk dat slechts een klein deel van een ICS daadwerkelijke traditionele IT betreft. Grofweg 20% van een gemiddelde ICS-omgeving gebruikt een conventioneel besturingssysteem zoals Windows of Linux. Lang niet alle traditionele IT-beveiligingstechnieken werken op dit deel, de meeste IT-beveiligingstechnieken, -processen en -methodes moeten worden aangepast op het betreffende ICS vanwege de speciale geïmplementeerde softwareomgevingen, protocollen en geïntegreerde besturingssystemen.

Gebruikelijke IT-beveiligingstechnieken knippen en plakken is dus absoluut geen goed idee. In sommige gevallen heeft zo'n oplossing geen effect of werkt de techniek niet, maar in het ergste geval kan een conventionele beveiligingsoplossing ernstige gevolgen hebben voor de veiligheid van mensen. Zelfs de betreffende 20% van een ICS vereist op maat gemaakte beveiliging.

Het goede nieuws is dat veel leveranciers van gespecialiseerde ICS-componenten de beveiliging van hun producten goed op orde hebben. Mensen gebruiken al decennialang kant-en-klare hard- en softwarecombinaties en dat kan in de meeste gevallen vrij veilig. Desalniettemin zijn er ICS-specifieke beveiligingscontrols voor netwerkzichtbaarheid en incident responsesystemen nodig bovenop de beveiligingsmaatregelen die fabrikanten leveren.

ANDERE AANVLIEGROUTE

De aard van de overige 80% van de geïntegreerde systemen in een ICS vereist wederom een fundamenteel andere aanvliegroute. Daar ligt dan ook gelijk een belangrijk verschil tussen ICS en traditionele IT; de meeste ICS-schakels hebben een extreem lage risicotolerantie. Zie het maar zo, de meeste reguliere netwerken worden met bijvoorbeeld anti-virussoftware beveiligd. Dat helpt doorgaans goed bij het weerhouden van een eventuele aanval. Maar zo'n oplossing kan ook onterecht een systeem, persoon of legitieme input aanzien voor beveiligingsdreiging en daarom buitensluiten, waardoor de werking van een overkoepelend ICS belemmerd kan worden.

> De meeste ICS-schakels hebben een extreem lage risicotolerantie

Deze lage risicotolerantie zie je ook terug in hoe systemen zijn ingericht, soms bijvoorbeeld berustend op verouderde software. Ik heb meermaals een ICS offline zien gaan doordat er verkeerd geïmplementeerde penetration testing werd gedaan op een systeem dat draaide op legacy software zoals Windows XP. Het kan zijn dat dergelijke oude systemen niet eens kunnen begrijpen dat er een nieuwe vorm van penetration testing wordt gehanteerd. Soms verzandt het scannen naar kwetsbaarheden hierdoor in een eindeloze

Zoek de delicate balans tussen kwetsbaarheid en de onderbreking van een systeem

cyclus. Wederom kan dit ongewilde gevolgen voor de veiligheid van een systeem hebben.

VERSCHILLEN IT EN ICS

Dat is de crux van de beveiliging van een ICS: veiligheid staat bij deze omgevingen voorop omdat de nadelige gevolgen enorm kunnen zijn. Daarom moet een ICS-beveiliger detectie prioriteren - geen preventie. Dit verlaagt de kans op vals-positieve blokkades van legitieme input van werknemers.
Maar een gebruikelijke endpointverdediging toegepast op individuele human machine interfaces (HMI) is niet genoeg om een overkoepelend ICS te beschermen. Daarom wordt er vaak gesproken over een 'netwerkbrede verdedigingslinie'; niet alleen individuele schakels, maar ook de connecties tussen die schakels moeten goed worden bestudeerd als ICS-specifieke controls, processen en technologieën zijn toegepast.
Een ICS-omgeving moet daarnaast doorgaans te allen tijde online zijn en mag niet stilgelegd worden. Dat is een van de redenen waarom sommige onderdelen van een ICS minder vaak geüpdatet worden; soms slechts één of twee keer per jaar, het standaardbeleid onder IT'ers is doorgaans een update iedere dertig dagen. ICS-componenten zijn gemaakt om in sommige gevallen decennia mee te gaan. Vanwege de vrij consistente aard van dergelijke systemen en de verhoogde isolatie van ICS-onderdelen komen grote veranderingen en daarmee nieuwe beveiligingsrisico's minder vaak voor. Tegelijkertijd kunnen de kosten van het offline halen van een systeem immens zijn, zowel financieel als immaterieel. Uiteraard wil een fabriek zo weinig mogelijk stilgelegd worden omdat ze hiermee omzet mislopen. Bij een ICS zijn de risico's veel groter en kost het meer tijd om handelingen te coördineren. Daarom moet er altijd een delicate balans gevonden worden tussen een onderbreking van een systeem en de waarschijnlijkheid dat een schakel kwetsbaar is en gebruikt kan worden voor een reële cyberaanval.

FUNDAMENTELE IT-PRINCIPES BLIJVEN

Gelukkig zijn er ook overeenkomsten tussen de traditionele IT-beveiliging en het beschermen van een ICS. Zoals bij alle grootschalige systemen zorgen gebruikers of medewerkers onopzettelijk voor aanvalsmogelijkheden, via HMI's kunnen aanvallers bij kwetsbare systemen komen. Maar deze interfaces zijn essentieel voor het goed functioneren van een systeem, bijvoorbeeld omdat technici via deze interfaces het algehele systeem in de gaten kunnen houden. Daarom is het net zoals in de gehele IT belangrijk dat authenticatie - bij voorkeur multi-factor - veilig gebeurt; individuen mogen nooit inloggegevens (met elkaar) delen en zouden met die gegevens alleen toegang moeten krijgen tot afgezonderde onderdelen van een systeem. Het splitsen van databases helpt tevens tegen het escaleren van een eventuele inbreuk in één systeem naar een ander; een zogenoemde laterale aanval van een gecompromitteerd IT-systeem naar een ICS-netwerk wordt dan moeilijker.

WEER- EN LEERBAARHEID

Met deze inherente risico's en uitdagingen lijkt het wellicht onmogelijk voor IT'ers om een ICS goed te beschermen, maar gelukkig zijn er in de praktijk ook voordelen. Technici en cyberbeveiligers zijn bijvoorbeeld per definitie altijd bezig met de veiligheid en betrouwbaarheid van een industrial control system, meer dan in veel traditionele IT-systemen. Dit zorgt voor een algeheel beveiligingsbewustzijn onder betrokkenen en daarmee voor een ingebakken weerbaarheid.
Voor een IT'er zijn die fundamentele beveiligingsprincipes van ICS's ook goed te leren. Hier zijn kort door de bocht drie kerneigenschappen voor nodig.
Je moet algemene IT-beveiligingskennis hebben, specifieke ICS-beveiligingstechnieken kennen en technische ervaring hebben binnen een specifiek ICS.
Je kunt als IT'er dan ook gemakkelijk een ICS-training volgen om de basisprincipes onder de knie te krijgen. Loop daarnaast eens een half jaartje mee met een monteur of technicus, leer een ICS kennen, leer de 'taal' spreken, leer hoe alle individuele systemen samenwerken. Op deze manier heb je binnen de kortste keren gespecialiseerde kennis van een ICS en kan een IT'er aan de slag met de beveiliging en verdediging van essentiële infrastructuren.

AUTEUR

DEAN PARSONS
is CEO en Principal Consultant van ICS Defense Force bij SANS.