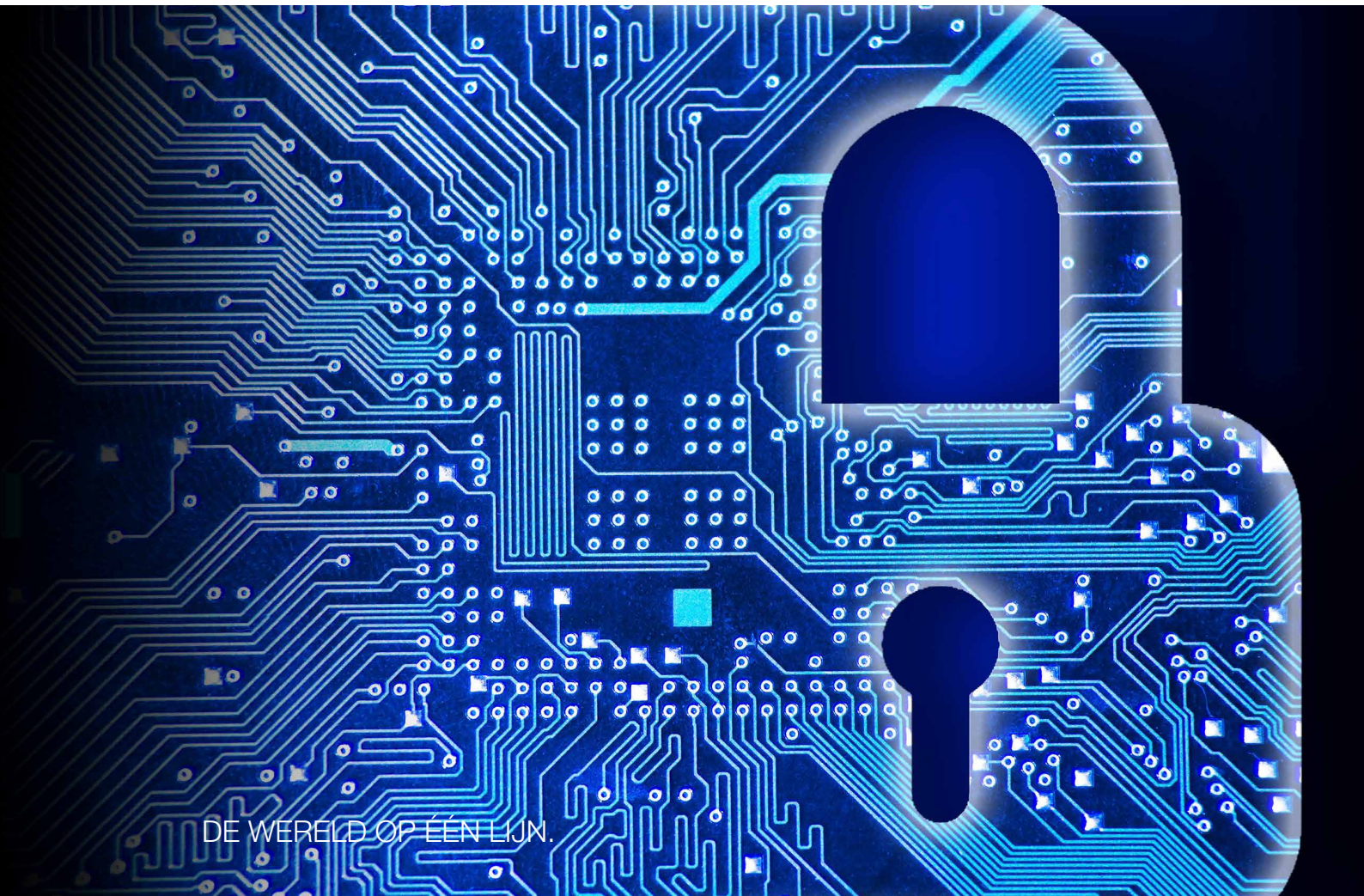
CYBERSECURITY STEEDS VAKER ONDERWERP VAN GESPREK BIJ HET BESTUUR VAN BEDRIJVEN

- Wist u dat industriële besturingssystemen gehackt kunnen worden?
- En weet u wat de gevolgen kunnen zijn van een dergelijk cyberincident op uw business?
- Wist u dat cybersecurity een ernstig veiligheidsprobleem kan worden? Of een juridisch probleem? Of een financieel probleem? Of alle drie gelijktijdig?

Signaleer indringers in uw productieomgeving in een vroeg stadium. Laat u door industriële automatiseringsexperts informeren over hoe u beleid kunt ontwikkelen voor de bescherming van uw productieomgeving en het vroegtijdig signaleren van indringers.

Toegevoegde waarde IEC 62443-normenreeks

Waarom zou u het wiel opnieuw uitvinden? U kunt voor het beveiligen van systemen en componenten die worden gebruikt in de industriële automatisering, gebruik maken van de IEC 62443 normenreeks. De normen zijn opgesteld door experts uit de industrie zelf en zijn van toepassing op processen, systemen en industriële componenten. De normen helpen u bij het opzetten van een effectief cybersecurity beleid voor industriële proces- en productieomgevingen en verkleinen de kans dat u zelf slachtoffer wordt van productieverlies door moedwillige of onbedoelde handelingen.



Voorbeelden

Enkele situaties waarbij de norm IEC 62443 u kan helpen:

- Verlenen van toegang aan een buitenstaander (zoals bijvoorbeeld een systeemintegrator) verlaagt uw beveiligingsniveau naar dat van de externe provider.

Als een hacker inbreekt in de systemen van deze provider, kan hij op die manier ook toegang krijgen tot uw eigen netwerk. Door totale bescherming in te stellen, helpt IEC 62443 om beleid te maken gericht op het voorkomen van ongeautoriseerde fysieke en digitale toegang tot systemen.

- Voorkomen van misbruik door een ontevreden werknemer

IEC 62443 helpt u bij het documenteren van de beschikbare en benodigde rechten van uw werknemers, zodat zij alleen toegang hebben tot systemen en informatie die nodig zijn voor de uitvoering van hun werkzaamheden. Ook helpt het om snel de toegang van oud-werknemers te blokkeren.

- Onderhouden van verouderde besturingssystemen

Oudere besturingen op uw productieterrein werken misschien nog steeds op verouderde applicaties die de leverancier niet meer ondersteunt, of ze draaien niet op de nieuwste versies van het besturingssysteem. IEC 62443 helpt om probleemoplossende maatregelen in te stellen.

- Vrijwaren van ramsomware

Ransomware kan de toegang tot de machine/applicatie vrijwaren. In 2017 zijn verschillende bedrijven geïnfecteerd met ransomware die hun productie met grote impact verstoorden met 100 miljoen euro schade tot gevolg. IEC 62443 helpt de activering van dergelijke ransomware

- Aanwezigheid van componenten met kwetsbare software in het industriële netwerk die onbedoelde externe penetratie van het netwerk veroorzaakt.

IEC 62443 helpt ervoor te zorgen dat er geen componenten met verouderde software draaien.

Wilt u de controle behouden over uw operationele systemen? Werk dan volgens IEC 62443!

Deze Elevator Pitch is een initiatief van het Platform Industriële Cyber Security. Neem voor meer informatie over IEC 62443 contact op met: IPCS@nen.nl

IPCS INDUSTRIEEL PLATFORM CYBER SECURITY

www.nen.nl/platformcybersecurity