De IT-security van de logistieke keten onder de loep

Als onderdeel van een logistieke keten bent u sterk afhankelijk van uw logistieke partners. Digitalisering maakt de keten efficiënter en geavanceerder. Tegelijkertijd zorgt dit echter ook voor een grotere afhankelijkheid van de continuering van de IT-processen. Om te voorkomen dat de beschikbaarheid van uw IT-processen wordt aangetast door cyberincidenten is het van belang dat uw IT-omgeving adequaat is beveiligd.

TNO onderzoekt momenteel, i.s.m. (branche)organisaties in de logistiek, de status van de IT-security van bedrijven in de logistieke keten. Het onderzoek leidt tot praktische handvatten voor bedrijven in de logistieke sector om de meest kritieke problemen in de keten te verhelpen en de cybersecurity te verbeteren. Het project wordt mede gefinancierd uit de Toeslag voor Topconsortia voor Kennis en Innovatie (TKI's) van het ministerie van Economische zaken.

Voor het onderzoek zijn wij op zoek naar bedrijven in de logistieke keten die zicht willen krijgen op het niveau van hun IT-security middels de uitvoer van een ‘ethische hack’.
De ‘ethische hack’ wordt uitgevoerd in de vorm van een gesimuleerde cyberaanval. Daarvoor wordt er een tool ontwikkeld die onderzoekt welke systemen door malware, zoals bijvoorbeeld het ‘WannaCry’ virus, aangetast kunnen worden. Deze tool wordt op het interne netwerk uitgevoerd. Vanzelfsprekend zal de tool geen daadwerkelijke schade toebrengen en worden uw systemen niet aangetast.

De ‘ethische hack’ verschaft inzicht in de mate waarop een malware-infectie de beschikbaarheid van IT-processen die van belang zijn voor de keten kan beïnvloeden. Nadat het onderzoek is afgerond, ontvangt u een overzicht van de resultaten die uit de ‘ethische hack’ op uw interne netwerk zijn voortgekomen. Het overzicht zal ook een (non-technische) interpretatie van de resultaten bevatten. Zo krijgt u een duidelijk beeld van de impact die een dergelijk incident op uw interne netwerk kan hebben en kunt u de verworven informatie gebruiken om het security-niveau te verhogen.

De resultaten van de ‘ethische hack’ worden door TNO anoniem verwerkt ten behoeve van het onderzoek dat het consortium met TNO uitvoert.

Naast de ‘ethische hack’ wordt een interview afgenomen door TNO-medewerkers om inzicht krijgen hoe cyber security (technisch) is georganiseerd. Het doel is mede inzicht te verkrijgen in ‘best practices’ ten aanzien van cyberveiligheid om uiteindelijk concrete handvatten op te kunnen stellen voor ondernemers om hun cyberweerbaarheid te vergroten. De handvatten zullen bestaan uit beveiligingsmaatregelen en 'best practices'.

Wat is het doel van de ‘ethische hack’?
In de Transport en Logistiek sector zijn bedrijven sterk afhankelijk van hun collega’s in de logistieke keten. Waar digitalisering deze keten efficiënter en geavanceerder maakt versterkt dit ook de afhankelijkheid van continuering in de IT-processen. Het doel van het onderzoek is inzicht verkrijgen in het IT-security niveau van de keten. De ‘ethische hack’ zoomt met name

in op de wijze waarop de digitale beschikbaarheid van de keten is gewaarborgd en op welke wijze deze beschikbaarheid kan worden aangetast door een malware-infectie.

Op welke manier wordt de 'ethische hack' uitgevoerd?
De 'ethische hack' wordt uitgevoerd in de vorm van een gesimuleerde cyberaanval. Daarvoor wordt er een tool ontwikkeld die onderzoekt welke systemen door malwarespreiding, zoals het 'WannaCry'-virus, aangetast kunnen worden. Deze tool zal op het interne netwerk worden uitgevoerd. Vanzelfsprekend zal de tool geen daadwerkelijke schade toebrengen en worden uw systemen niet aangetast.

Wie voert de 'ethische hacks' uit?
De 'ethische hacks' worden uitgevoerd door deskundige IT-security specialisten van REQON Security. Zij ontwikkelen de tool en testen deze grondig in hun eigen omgeving. Vervolgens wordt deze bij de deelnemende partijen uitgevoerd. Uiteraard zijn zij bereid om een geheimhoudingsverklaring (NDA) te ondertekenen.

Wie neemt de interviews af?
De interviews worden afgenomen door medewerkers van TNO. Uiteraard zijn ook zij bereid om een geheimhoudingsverklaring (NDA) te ondertekenen.

Wat gebeurt er met de gegevens uit de hacks en de interviews?
De informatie, voortkomend uit de hacks en de interviews, wordt door REQON Security en TNO geanonimiseerd. Vervolgens worden, met behulp van de informatie uit alle hacks en interviews, 'best practices' en praktische handvatten opgesteld ten behoeve van het verbeteren van de cybersecurity van de gehele sector. Deze worden door de brancheverenigingen verspreid. De naam van uw bedrijf wordt hierin uiteraard niet genoemd.

Wie zitten er in het consortium en welke informatiekrijgen zij?
Het consortium bestaat uit TNO, Transport en Logistiek Nederland (TLN), SmartPort, Air Cargo Netherlands (ACN), Havenbedrijf Rotterdam, Cargonaut, REQON Security en Computest. Alleen TNO en REQON Security zien de resultaten uit de 'ethische hack' en het interview gekoppeld aan de naam van uw bedrijf. De andere consortiumpartners krijgen alleen geanonimiseerde informatie.

Welke kosten zijn er aan de deelname verbonden en wat levert het u op?
Om deel te nemen aan het onderzoek betaalt u éénmalig een bedrag van 1.500 euro. Voor dit bedrag wordt de 'ethische hack' op uw interne netwerk uitgevoerd. Van de resultaten ontvangt u een overzicht, aangevuld met een (non-technische) interpretatie. Zo krijgt u een duidelijk beeld van de impact die een dergelijk incident op uw interne netwerk kan hebben. U kunt de verworven informatie gebruiken om het security-niveau te verhogen.

Wat wordt er van u verwacht?
Om de uitvoering van de 'ethische hack' te begeleiden, dient er een interne IT-medewerker (netwerkbeheerder of systeembeheerder met security affiniteit) aanwezig te zijn. Tevens wordt er door een medewerker van TNO een interview bij de IT-medewerker afgenomen

over het securitybeleid van uw organisatie. Daarnaast wordt u verzocht een vrijwaringsverklaring te ondertekenen die REQON Security vrijwaart om zo het onderzoek op uw systemen uit te kunnen voeren.

Meer informatie
Voor meer informatie over deelname kunt u contact opnemen met de afzender van dit bericht.