

Cyberveiligheid en de supply chain

Potentiële dreigingen en hoe u die afslaat

kaspersky.nl
www.securelist.com

kaspersky BRING ON THE FUTURE

Voorwoord

Cybercriminelen zijn steeds geraffineerder geworden in het uitbuiten van organisatorische silo's, beveiligingsgaten als gevolg van werken op afstand en de supply chain-crisis, om de veiligheid en beveiliging van kritieke systemen te ondermijnen. Dergelijke gerichte aanvallen kunnen hele netwerken van organisaties in de supply chain beschadigen en ontwrichten, met reputatieschade en verwoestende financiële verliezen tot gevolg.

Doeltreffende beveiliging tegen cyberrisico's kan ontmoedigend zijn, aangezien kwetsbaarheden vaak inherent zijn aan of worden geïntroduceerd en uitgebuit op elk punt in de supply chain. Een recente reeks in het oog springende en zeer schadelijke aanvallen op bedrijven - zoals bij SolarWinds en Colonial Pipelines - heeft in feite aangetoond dat aanvallers de intentie en het vermogen hebben om kwetsbaarheden in de beveiliging van de supply chain uit te buiten, waardoor wereldwijde verstoringen ontstaan in de levering van dagelijkse goederen en diensten.

Dit kan gevolgen hebben voor overheden, ondernemingen en mensen. Een aanval op een kruidenierssketen kan de tijdelijke sluiting van supermarkten tot gevolg hebben, of een virus kan via een software-update op miljoenen pc-gebruikers worden losgelaten, of een aanval op systemen voor gezondheidszorg of openbare nutsvoorzieningen kan de levering van deze essentiële diensten verstoren. Wat de recente aanvallen gemeen hebben, is de manier waarop ze zich gedragen. Kwaadwillende actoren richten zich op softwareleveranciers of grote onderling afhankelijke bedrijven om achterdeurtoegang te krijgen tot hun systemen en die van hun klanten. Zo kunnen de cybercriminelen in één keer duizenden systemen besmetten en een domino-effect veroorzaken.

Ondanks de complexiteit van de risico's in de supply chain, mogen we niet bij de pakken neerzitten. Deze trend is reëel en neemt toe, en zet bedrijven van elke omvang ertoe aan de weerbaarheid van hun supply chain dringend onder de loep te nemen, te beschermen en te verbeteren. Gezien de globalisering en onderlinge verwevenheid van supply chains is er behoefte aan de ontwikkeling van basisprincipes, technische normen en een solide basis voor cyberbeveiliging om een consistent niveau van bescherming tegen datalekken door derden te waarborgen.

Zoals in ons rapport wordt benadrukt, is het van essentieel belang geworden dat organisaties beschikken over goed gedocumenteerde, begrijpelijke en geoefende plannen en processen. Op die manier staan ze klaar om te reageren op het moment dat zich een cyberincident of -crisis voordoet en om snel te kunnen herstellen, met name in de context van herstel na een pandemie.

Tim de Groot
Territory Manager Benelux en Nordics bij Kaspersky



Contents

Voorwoord 2

Inleiding 4

Methodiek 5

Belangrijkste bevindingen (Benelux) 5

Risico's van de supply chain 6

Cyberverzekering 7

Tikkende tijdbom 8

Detecteren is beter dan genezen: supply chain-aanvallen zien en voorkomen 9

CHECKLIST – Wat kunt u doen om uw bedrijf te beschermen? 10

Conclusie 11

Inleiding

De moderne wereld functioneert via een web van digitale verbindingen, waarin elke interactie een potentiële kans voor cybercriminelen vormt.

In 2021 gingen cybercriminelen geraffineerder te werk dan ooit door organisatorische silo's, thuiswerkers en de crisis in de supply chain uit te buiten om zo de veiligheid en beveiliging van kritieke systemen te ondermijnen. De pandemie heeft de groeiende complexiteit en hevigheid van cyberaanvallen alleen maar versterkt.

Supply chain-risico's en risico's van derden kwamen het afgelopen jaar in het nieuws met de **SolarWinds** en **Colonial Pipeline**-aanvallen, die lieten zien hoe kwaadwillenden een enorm aantal organisaties kunnen bereiken via één schakel in de supply chain.

> "Cyberaanvallen worden steeds geraffineerder en samenwerking is cruciaal om de strijd tegen een goed georganiseerde groep tegenstanders die over ruime financiële middelen beschikken te kunnen winnen. CISO's denken misschien dat ze heel goed bezig zijn door de juiste controlemechanismen en ecosystemen op te tuigen om hun organisatie te beschermen, maar hun tegenstanders zitten heel ergens anders en richten zich op de zwakste schakel in de supply chain."
>
> **Jitender Arora,**
> **Chief Information Security Officer bij Deloitte VL**

De beveiliging van een organisatie kan nog zo sterk zijn, één zwakke schakel in de supply chain kan een bedrijf op de knieën brengen. Uit ons rapport bleek dat bedrijven van alle grootten en in alle sectoren te weinig aandacht besteden aan cyberveiligheid. Hoewel bijna dan driekwart (72%) aangeeft cyberveiligheidsdreigingen prioriteit boven herstel van de pandemie te stellen, blijkt een verontrustend aantal te gemakkelijk te denken over hun eigen cyberveiligheid en die van hun supply chain.

Zowel grote als kleine bedrijven kunnen het zich niet veroorloven op dit gebied achterover te leunen. Terwijl organisaties zich richten op het oplossen van problemen met de supply chain, zoals het lossen van containerschepen en het oplossen van personeelstekorten terwijl de kosten moeten worden gedrukt, misbruiken cybercriminelen een hyper-verbonden digitaal toeleveringsnetwerk voor nieuwe aanvalsvectoren.

Ons rapport onderstreept de noodzaak voor bedrijven om de referenties van leveranciers nauwkeurig te onderzoeken als onderdeel van het standaard due diligence- en aanbestedingsproces, omdat ze anders zichzelf nietsvermoedend blootstellen aan een cyberveiligheidsramp.

Met de **verwachte toename** in 2022 van aanvallen op de supply chain-IT, neemt de druk op bedrijven toe om te verzekeren dat hun leveranciers tegen cyberaanvallen zijn beschermd. Bij Kaspersky zijn we ervan overtuigd dat de pandemie en het domino-effect daarvan in de supply chain het cyberdreigingslandschap heeft veranderd, en het is essentieel dat organisaties stappen zetten om deze nieuwe uitdagingen het hoofd te bieden. Bedrijven zouden moeten verzekeren dat ze alleen gegevens delen met betrouwbare derden en van hun leveranciers dezelfde beveiligingsnormen verlangen als zijzelf hanteren.

Dit rapport heeft tot doel om technologiele-veranciers, service providers, organisaties en professionals op het gebied van beveiliging inzicht te geven in het groeiende dreigingslandschap voor de supply chain. Het biedt ook aanbevelingen voor het oplossen en beperken van potentiële inbreuken op de cyberveiligheid van het bedrijf zelf en diens supply chain.



Methodiek

In november en december 2021 voerde Arlington Research een onderzoek uit onder 240 C-suite, middenkader (directieniveau en hoger) en senior managers met beslissingsbevoegdheid of gezamenlijke beslissingsbevoegdheid op het gebied van cyberveiligheid, IT en informatiebeveiliging, onder zowel kleine en middelgrote bedrijven (met een jaaromzet van minder dan £/€ 100 mln) als grote bedrijven (met een jaaromzet van meer dan £/€ 100mln). 150 enquêtes werden uitgevoerd in het VK (onder 100 kleine en middelgrote bedrijven en 50 grote bedrijven) en 90 enquêtes werden uitgevoerd in de Benelux (onder 75 kleine en middelgrote bedrijven en 15 grote bedrijven).

Belangrijkste bevindingen (Benelux)

- 62% van de organisaties maakt zich meer zorgen over cyberveiligheidsdreigingen dan over herstel van de pandemie (56%) en de stijgende kosten van grondstoffen (49%). Vermeldenswaardig is dat bijna een kwart (23%) zich zeer grote zorgen maakt over cyberveiligheidsdreigingen.

- 39% van de respondenten is het er 'zeer mee eens' dat ze 'al het mogelijke hebben gedaan om risico's van derden te beperken' voor de organisatie. Eén op de tien organisaties gaf echter tijdens de crisis in de supply chain minder prioriteit aan cyberveiligheid, ondanks het feit dat 27% een toename van het aantal aanvallen in de afgelopen 12 maanden meldde.

- Bijna twee derde (65%) van de organisaties is ervan overtuigd dat hun bedrijf over voldoende up-to-date hardwarematige en softwarematige IT-beveiliging beschikt, maar 12% heeft niet alle benodigde middelen en kennis in huis om op elk cyberveiligheidsincident te kunnen reageren.

- Iets minder dan drie op de tien beslissers (29%) is het er zeer mee eens dat zij erop vertrouwen dat hun IT-beveiligingsproviders hun organisatie zullen helpen bij een cyberveiligheidsincident.

- Bijna een kwart van de organisaties (23%) heeft oplossingen van derden voor risicobeheersing, ondanks dat twee derde (66%) in de afgelopen 12 maanden een aanval heeft meegemaakt.

- 57% van de organisaties geeft aan dat hun organisatie nooit zou samenwerken met een bedrijf waar een gegevenslek is voorgekomen, en toch is slechts 66% van de beslissers op het gebied van IT-beveiliging ervan overtuigd dat ze de IT-beveiliging van nieuwe leveranciers of partners zorgvuldig onder de loep nemen voordat ze een contract ondertekenen, terwijl minder dan een op de tien (8%) expliciet aangeeft dit niet te doen.

Risico's van de supply chain

In elke sector geldt dat een bedrijf op de knieën kan worden gebracht als de zwakste schakel in een supply chain wordt uitgebuit.

Een kwetsbaarheid op de ene plek kan een grote uitwerking hebben op een andere plek, of dat nu via misbruik van persoonsgegevens of betaalgegevens gebeurt. Cyberaanvallen leiden tot grote financiële schade, diefstal van intellectueel eigendom, psychische spanningen, verstoring van services en eigendommen en risico's voor infrastructuur. De gevolgen van zo'n aanval kunnen een bedrijf grote reputatieschade toebrengen.

In zijn jaarlijkse rapport (CSAN 2021) geeft de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) aan dat tussen maart 2020 en maart 2021 er talloze cyberincidenten waren in of met betrekking tot Nederland. Met name aanvallen op supply chains zijn in de afgelopen maanden in aantal, schaal en complexiteit toegenomen.

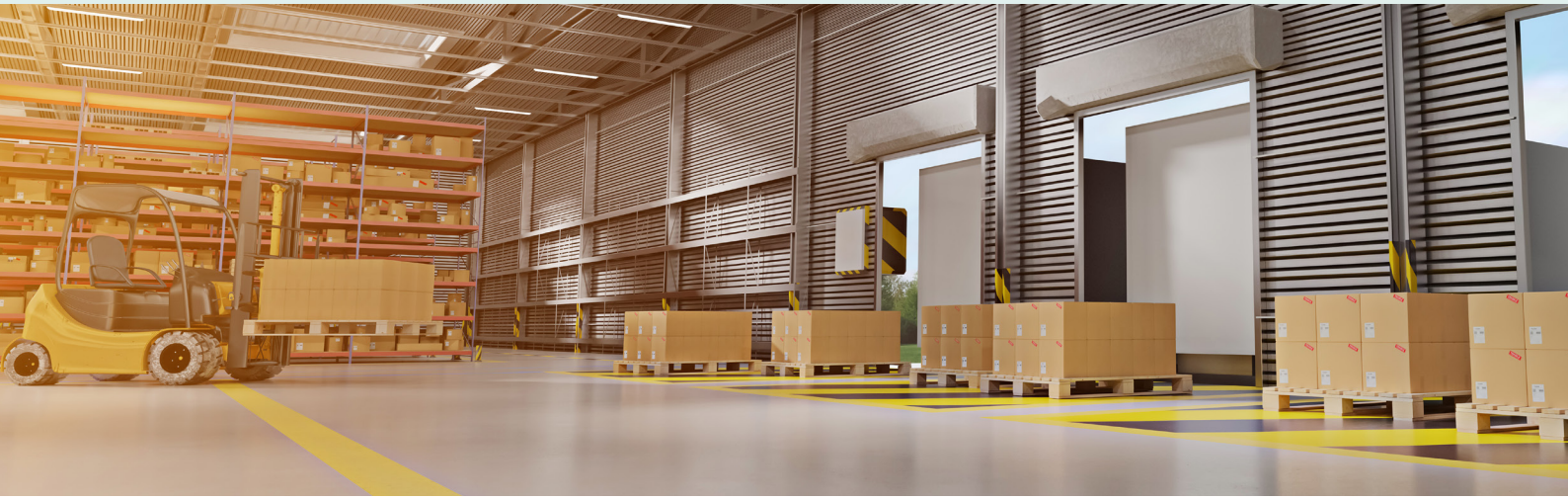
Veel Nederlandse bedrijven in verschillende sectoren en branches hebben onder aanvallen op de supply chain te lijden gehad. Zo kwamen bijvoorbeeld Nederlandse supermarkten zonder zuivel te zitten nadat een van de grootste logistieke dienstverleners van het land door een ransomwareaanval werd getroffen, waardoor de leveringen ernstig werden verstoord terwijl het team het cyberincident probeerde op te lossen.

En recent nog meldden grote olieterminals bij enkele van de grootste havens van Europa dat ze het slachtoffer van een cyberaanval waren geworden op een moment dat de energieprijzen toch al extreem hoog waren. In Nederland, België en Duitsland kregen olie-installaties te maken met ransomwareaanvallen die tot grote problemen konden leiden voor de olietoevoer in de regio. Het effect van dergelijke aanvallen kan groot zijn en in het hele land gevoeld worden: tankstations krijgen bijvoorbeeld geen brandstof meer geleverd, waardoor auto's en vrachtwagens niet meer kunnen tanken.

Ook al geeft bijna twee derde (62%) van de bedrijven uit ons onderzoek aan dat cyberveiligheids-dreigingen de hoogste prioriteit hebben, meer dan een op de tien (12%) zegt onvoldoende middelen en kennis in huis te hebben om adequaat op een cyberveiligheidsincident te kunnen reageren, en slechts 39% van de respondenten is het er 'zeer mee eens' dat ze al het mogelijke hebben gedaan om risico's van derden in hun organisatie te beperken.

Behoorlijk verontrustend is ook dat ondanks dat 27% van de bedrijven in de afgelopen 12 maanden meer cyberaanvallen heeft meegemaakt – stijgend tot 60% in de categorie grote bedrijven[1] – zegt 10% dat ze niet de nodige uitgaven doen om cyberveilig-heidsincidenten te voorkomen.

[1] Groot bedrijf gedefinieerd als met een jaaromzet van meer dan € 500 miljoen



Cyberverzekering

In een wereld met uiteenlopende cyberdreigingen die bovendien voortdurend evolueren, kan een cyberverzekering organisaties na een aanval weer op de been helpen.

Toch blijkt uit ons onderzoek dat ondanks dat bijna een kwart van de respondenten in de Benelux (24%) de noodzaak aangaf om in risicobeheersings-oplossingen van derden te investeren, een op de vijf (20%) denkt dat risicobeheersingsoplossingen van derden geen prioriteit hebben, hoewel ze wel nuttig kunnen zijn.

Dat aantal was hoger (30%) bij degenen die willen investeren in een cyber/bedrijfsbeschermings-verzekering, hoewel meer dan een op de tien (11%) aangaf daarin geen interesse te hebben.



"De handen ineenslaan met een cyberverzekeringsbedrijf is niet alleen nuttig om uw bedrijf te laten terugveren na een aanval, maar zo'n bedrijf kan ook helpen hiaten in uw beveiliging te identificeren en is een uiterst waardevolle manier om risico's te verkleinen en te elimineren. En dat laatste is belangrijk, want anders bestaat het gevaar dat een cyberverzekering wordt gezien als een manier om tegen de gevolgen van een aanval te beschermen, in plaats van deze te gebruiken als onderdeel van de risicobeoordelings- en beheersingsstrategie."

David Emm
Principal Security Researcher,
Global Research & Analysis Team



Tikkende tijdbom

De pandemie verscheen bij de meeste organisaties twee jaar geleden voor het eerst op de radar en de supply chains hadden er zwaar onder te lijden.

Hoewel de meerderheid zei dat cyberveiligheid een grotere prioriteit is geworden gezien de huidige crisis in de supply chain, is het verontrustend dat 10% in de afgelopen 12 maanden cyberveiligheid minder prioriteit is gaan geven.

Cyberaanvallen en gegevenslekken kunnen een organisatie veel schade toebrengen wat betreft merkreputatie, herstelkosten, omzetverlies en andere onkosten. Dit wordt ondersteund door ons onderzoek waaruit blijkt dat bijna drie op de vijf organisaties (57%) zegt nooit te willen samenwerken met een bedrijf waar een gegevenslek heeft plaatsgevonden, wat het belang van gegevensbeveiliging voor toekomstige zakelijke kansen onderstreept.

Bij een substantieel aantal organisaties komt de boodschap echter niet aan dat een risico in de supply chain invloed kan hebben op hun bedrijfsresultaat door het mislopen van nieuwe klanten: 20% van de organisaties geeft aan dat ze van potentiële nieuwe klanten geen vragen over hun beveiliging verwachten.

Geruststellend is dat iets minder dan twee derde (63%) aangeeft altijd cyberveiligheid in nieuwe contracten met leveranciers of partners op te nemen, hoewel een klein percentage (12%) dat nog steeds niet doet, met name in het segment kleine en middelgrote bedrijven, met nog eens 14% die het niet eens is met de aanname dat de IT-beveiliging van leveranciers of partners belangrijk is voor hun bedrijfscontinuïteit.

Nu het aantal cyberaanvallen toeneemt, is het belangrijker dan ooit dat organisaties kwetsbaarheden in hun supply chain identificeren. Aanvallers zijn opportunistisch en grijpen elke gelegenheid aan.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCSC) adviseert om met leveranciers om de tafel te gaan en duidelijke afspraken met hen en hun onderaannemers te maken. Bestaande normen en richtlijnen op basis van risicobeheer dienen te worden gevolgd bij de aanschaf van producten en services. In dat verband zouden organisaties ook beveiligingsvereisten voor leveranciers in hun aankoopprocessen moeten opnemen.

"Als u op de een of andere manier een vertrouwensrelatie met een entiteit hebt, hebt u te maken met risico's van derden. Dat risico kan komen van een leverancier, de verhuurder van uw kantoor, softwareproducenten, een app op de smartphone van uw personeel, enzovoort."

"Een van de grootste uitdagingen voor bedrijven bij het uitvoeren van een risicobeoordeling van derden, is dat ze geneigd zijn een kader te gebruiken dat op hun individuele behoeften is afgestemd. We adviseren om alle afdelingen in uw organisatie bij het proces te betrekken om te helpen risico's in de supply chain te identificeren. Uw financiële team kan bijvoorbeeld de leverancier controleren op certificeringen, witwassen en fraude, terwijl uw marketing- en communicatieteam kan kijken naar ongunstige berichtgeving in de media. Soms kunt u om een eerste penetratietest vragen om het beveiligingsniveau van een infrastructuur te beoordelen en als u een stap verder wilt gaan, kunt u een volledige audit uitvoeren."

Vladimir Krupnov
Threat Intelligence Lead bij Revolut Bank

Detecteren is beter dan genezen: supply chain-aanvallen zien en voorkomen

Bij een supply chain-aanval wordt een organisatie doelwit door het infiltreren van of aanvallen via een externe leverancier. Als een van deze entiteiten een matige cyberveiligheidsbescherming heeft, kunnen kwaadwillenden via die organisatie de hele supply chain binnenkomen. Het risico kan sterk variëren en maakt het dreigingsoppervlak van een organisatie nog complexer.

De waarschijnlijke impact van cyberaanvallen varieert per speler in de supply chain. Er is echter specifiek gedrag dat een bedrijf kwetsbaarder voor een cyberaanval kan maken. Denk daarbij onder meer aan een zwakke algehele internet- of IT-beveiliging, een zwak wachtwoordbeleid, software niet up-to-date houden, slechte systeemmonitoring en inadequate mechanismen voor toegangscontrole. Geen of slechte beveiligingsmaatregelen vergroten het risico van een cyberaanval aanzienlijk.



"Grotere organisaties kunnen kleine en middelgrote bedrijven die heel goed zijn in hun core business, maar niet in beveiliging, de helpende hand reiken met advies en begeleiding om ze te ondersteunen in hun behoeften en de risicobeheersing te verbeteren. Wat we vaak vergeten, is dat we het hebben over wereldwijd opererende aanvallers die heel subtiel en uiterst georganiseerd te werk gaan. Daarom moeten we de handen ineenslaan en zelf ook veel georganiseerder worden. Een manier waarop we onze supply chain en externe leveranciers, met name kleine en middelgrote bedrijven, echt kunnen helpen, is door onze best practices met hen te delen en hen te ondersteunen."

Jitender Arora
Chief Information Security Officer bij Deloitte VL

"Iets wat vaak over het hoofd wordt gezien, is dat bedrijven ook voortdurend in de gaten moeten houden wanneer hun apparatuur en software het einde van de levenscyclus (EOL) bereikt, met name wanneer die status dichterbij komt. Alle apparatuur die de EOL-fase heeft bereikt, wordt niet meer officieel ondersteund. Dat betekent dat er geen updates en patches meer beschikbaar zullen zijn, waardoor ze kwetsbaarder worden voor een gerichte aanval."

Jornt van der Wiel
Senior security researcher voor het Global Research and Analysis Team bij Kaspersky



CHECKLIST – Wat kunt u doen om uw bedrijf te beschermen?

› **Stel vast wie uw leveranciers zijn**
De belangrijkste stap voor elke organisatie – en één die vaak wordt overgeslagen. Maak een overzicht van bij wie u producten en services afneemt en waar uw organisatie zich bevindt in de supply chain, zodat u een kaart met potentiële risico's kunt opstellen.

› **Stel vast wat er moet worden beschermd**
Als u via een supply chain wordt aangevallen, betekent dat meestal dat een service of applicatie die u al enige tijd gebruikt is geïnfecteerd. Elk apparaat in het bedrijf met internettoegang moet worden beschermd, waaronder computers, servers, mobiele telefoons, enzovoort. Hoewel het netwerk moet worden beschermd tegen opportunistische aanvallen voor snel geld, is het ook cruciaal om technologie in te zetten die waarschuwt bij vroegtijdige tekenen dat kwaadwillenden het systeem proberen te infiltreren om cyberspionage te plegen.

› **Stel vast wat het risico voor uw organisatie is**
Denk na over potentiële kwetsbaarheden waardoor aanvallers de organisatie kunnen binnendringen. Dit moet zowel beleid en processen omvatten als technologie. Sterker nog, dit moet zaken omvatten waarover u geen rechtstreekse controle hebt, zoals producten en services die door derden worden geleverd. Dat kunnen applicaties zijn, code die op uw systemen wordt uitgevoerd en externe toegang van een derde partij tot het netwerk.

› **Evalueer de processen en beveiliging van leveranciers**
U dient een grondige audit uit te voeren van de cyberveiligheid en risicobeheersingsplannen van uw leveranciers en het feit of zij al dan niet hun eigen leveranciers op dezelfde wijze evalueren. Dat zou een goede indicatie moeten geven van de risico's en welke processen zorgvuldig moeten worden beheerd.

› **Onderneem actie**
Stel een robuust incidentresponsplan op met heldere doelstellingen en creëer een speciaal team dat goed is voorbereid om hierop te acteren. Dit plan moet tevens stappen voor risicobeperking omvatten in het geval dat er een aanval plaatsvindt.

› **Gebruik de middelen die je ter beschikking staan**
Het Nationaal Cyber Security Centrum biedt organisaties verschillende handvatten om zich tegen cyberaanvallen te beschermen. In de Handreiking Cybermaatregelen vinden organisaties een stappenplan waarmee zij hun digitale veiligheid kunnen verbeteren. Daarnaast staan er linkjes naar andere publicaties met handvatten om de weerbaarheid van uw organisatie tegen cyberaanvallen te vergroten.

Conclusie

Ons onderzoek laat zien dat het voor organisaties cruciaal is om robuuste programma's op te zetten voor het beheersen van zowel bekende als onbekende risico's vanuit de supply chain. Bovendien zouden leiders moeten onderkennen dat risicobeheersing meer is dan het opzetten van processen en governancemodellen en ook vraagt om een cultuurverandering en een andere denkwijze, waarbij leveranciers verderop in de supply chain worden geholpen met het implementeren van robuuste veiligheidsmechanismen.

Door cyberveiligheid op deze manieren te benaderen, vergroten organisaties hun kansen om verstoringen van de supply chain en daaruit voortkomende crises te minimaliseren, en tegelijk optimaal profijt te hebben van hun supply chain-strategieën.

In reactie op de uitdagingen rond risico's in de supply chain en om bedrijven die specifieke cyberveiligheidsbescherming nodig hebben te helpen, hebben specialisten van Kaspersky **Interactive Protection Simulation (KIPS)** ontwikkeld. Dit is een oefening waarin beslissers en IT-beveiligingsteams van bedrijven en overheidsinstanties in een gesimuleerde bedrijfsomgeving een reeks onverwachte cyberdreigingen het hoofd moeten bieden, terwijl ze proberen maximale winst te behalen en het vertrouwen van anderen in hun bedrijf te behouden.

Het idee is om een verdedigingsstrategie tegen cyberaanvallen op te stellen door te kiezen uit de beste proactieve en reactieve beheermiddelen die ze ter beschikking staan. Elke keer dat een team reageert op de gebeurtenissen, verandert het verhaal en elke verandering beïnvloedt hoeveel winst het bedrijf maakt of misloopt. De teams wegen technische, zakelijke en veiligheidsprioriteiten af tegen de kosten van een realistische cyberaanval. Ze analyseren gegevens en nemen strategische beslissingen op basis van onzekere informatie en beperkte middelen. Dat klinkt niet alleen realistisch, dat is het ook. Elk scenario is namelijk gebaseerd op echte gebeurtenissen.

Ga voor meer informatie over Kaspersky Interactive Protection Simulation naar:

Kaspersky Expert Security

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Technologies at glance: www.kaspersky.com/TechnoWiki
Threat Intelligence Portal: opentip.kaspersky.com
Awards and recognitions: media.kaspersky.com/en/awards
www.kaspersky.com/fraudprevention

www.kaspersky.nl



2022 AO KASPERSKY LAB. ALL RIGHTS RESERVED.
REGISTERED TRADEMARKS AND SERVICE MARKS ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS.