Cybersecurity en bedreigingen vanuit statelijke actoren

Case study China

—

November 2022

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

US And UK Security Services Warn Of China Risks

Emma Woollacott Senior Contributor

Follow

Jul 7, 2022, 05:34am EDT

MI5 Director General Ken McCallum (left) and FBI Director Christopher Wray at a joint press ...

AIVD waarschuwt hightech-bedrijven tegen Chinese spionage

De AIVD heeft spionage door Chinese en Russische inlichtingendiensten bij Nederlandse technologiebedrijven ontdekt en voorkomen. De bedrijven zijn erover ingelicht. De AIVD acht de dreiging van digitale aanvallen in ons land groot.

NOS Nieuws • Maandag 7 februari 2022, 08:14 •
Aangepast maandag 7 februari 2022, 12:41

'Spionnen uit China en Rusland stelen via LinkedIn bedrijfsgeheimen'

AIVD: Chinese geheime dienst hackt gevoelige info in Nederland

UPDATE **De Chinese geheime dienst is betrokken bij het hacken van overheidsinstanties en bedrijven in Nederland. APT10, een hackersgroep gelinkt aan het Chinese ministerie voor Staatsveiligheid, wordt verantwoordelijk gehouden voor vele hackpogingen in een aantal westerse landen, waaronder Nederland.**

Sanne Schelfaut 19-01-19, 15:46 Laatste update: 19-01-19, 20:27

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

"China almost certainly is capable of launching cyber attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems."

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

De presentatie is geen uitdrukking van (persoonlijke) politieke overtuigingen

De bevindingen zijn slechts het resultaat van een open bronnen onderzoek door KPMG NL

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

ASIA

China Is Decoupling And Setting Its Own Economic Order

Vasuki Shastry Contributor

I write about Asian economics and technology news.

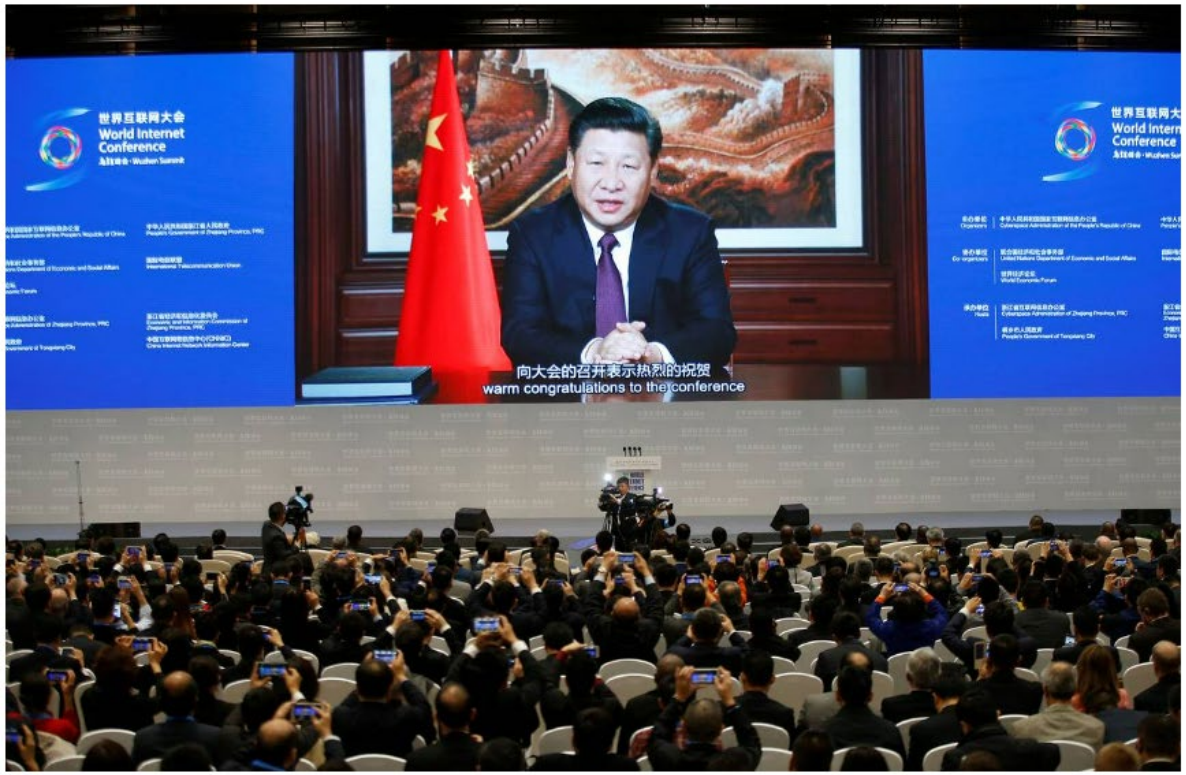
Follow

Sep 3, 2021, 08:15am EDT

TECH

China's Xi Jinping Opens Tech Conference With Call for 'Cyber Sovereignty'

President makes remarks by video to state-run conference aimed at pushing Beijing's version of the web



Xi Jinping spoke by video at the Wuzhen World Internet Conference.

PHOTO: ALY SONG/REUTERS

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Interessegebieden van China

Alternatieve energie	Zonne-energie, windturbines, hybride/elektrische auto's
Biotechnologie	Biofabricage, biofarmaceutische producten, genetisch gemodificeerde organismen, behandeling van besmettelijke ziekten, geavanceerde vaccins en geneesmiddelen
Defensie - lucht- en ruimtevaart en luchtvaartsystemen	Bewapening, maritieme systemen, radar, optica, ruimte-infrastructuur en verkenningstechnologie
High-end Manufacturing	Chemische productie, geavanceerde robotica, vliegtuigmotoren, hoogwaardige composietmaterialen, apparatuur voor geïntegreerde circuitfabricage en assemblagetechnologie
Emerging Technology	Kunstmatige intelligentie, Big data-analyse, geavanceerde computerchips, netwerkapparatuur, quantum-computing en communicatie en de benodigde zeldzame aardmetalen

KPMG

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Document Classification: KPMG Public

Colin Kahl, undersecretary of defense for policy.

U.S. Department of Defense. "Official Talks DOD Policy Role in Chinese Pacing Threat, Integrated Deterrence." Accessed February 8, 2022.

"The country's (red: China) offensive cyber capabilities rival or exceed that of the United States"

and

"China has built asymmetric capabilities that the United States is constrained against developing by international or domestic law."

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Tianfu Cup

Organizers (in random order)

奇安信 · 赛博昆仑 CYBER KUNLUN · HUAWEI · Baidu 百度 · Alibaba Group 阿里巴巴集团 · 360

清华大学 网络科学与网络空间研究院 · 中国科学院 信息工程研究所 · CIC 工信安全 · NSFOCUS · 天融信 TOPSEC · 启明星辰

永信至诚 · AsiaInfo 亚信安全 · 成都天投 CHENGDU TIANFU NEW AREA INVESTMENT GROUP CO.,LTD

Co-organizers (in random order)

安恒信息 DAS-Security · CETC 中国网安 CHINA CYBER SECURITY · 知道创宇 · 四叶草安全 Cover Sec · 智联招聘

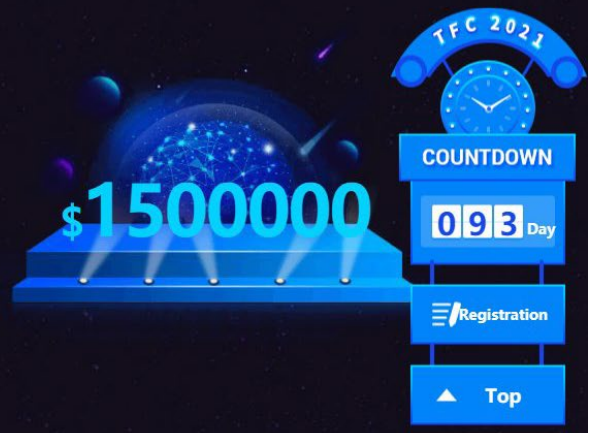
© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

JOIN THE EVENT

International Cybersecurity Contest

With the target of gradually creating China' s own "Pwn2Own", Tianfu Cup International PWN Contest will have three independent and parallel events: the original vulnerability demonstration and recurrence contest, the product Contest, and the system Contest. All teams are required to use original vulnerabilities to hack the given subject. The total bonus of the contest will reach up to 1.5 million US dollars in a bid to deliver a feast of cyber security technologies.

Competition Rules | Contest Topic



天府杯 TIANFUCUP 赛程 TIMETABLE

11-16 DAY 1

Status	Time	Team	Target
Failed	09:15-10:55	SDC Dreamcatcher	Microsoft Edge
Failed	09:15-10:55	EPL Team	Microsoft Edge
Gave Up	---	Tortollan	Microsoft Edge
Succeeded	09:15-10:55	ddd Team	Microsoft Edge
Succeeded	09:15-10:55	·	Microsoft Edge
Succeeded	09:15-10:55	360Vulcan	Microsoft Edge
Failed	10:55-11:55	EPL Team	Chrome
Succeeded	10:55-11:55	0x34567a61	Chrome
Succeeded	10:55-11:55	ddd Team	Chrome
Gave Up	---	360Vulcan	Chrome
Succeeded	12:15-12:35	StackLeader	Safari
Gave Up	---	EPL Team	Safari
Gave Up	---	ddd Team	Safari
Gave Up	---	360Vulcan	Safari
Succeeded	13:00-14:00	HAC	D-Link DIR-878
Succeeded	13:00-14:00	StackLeader	D-Link DIR-878
Gave Up	---	HeapLeader	D-Link DIR-878

11-16 DAY 1

Status	Time	Team	Target
Succeeded	13:40-14:00	360Vulcan	Microsoft Office (...
Succeeded	14:00-15:00	bit-STARLabs	Adobe PDF Reader
Succeeded	14:00-15:00	StackLeader	Adobe PDF Reader
Gave Up	---	HeapLeader	Adobe PDF Reader
Gave Up	---	Tortollan	Adobe PDF Reader
Gave Up	---	360Vulcan	Oracle VirtualBox
Failed	15:20-16:20	Beijing Onlookers	TP-Link WDR7660
Gave Up	---	FPXnb!!!	TP-Link WDR7660
Gave Up	---	0x34567a61	TP-Link WDR7660
Failed	15:20-16:20	Tianjun Team	TP-Link WDR7660
Succeeded	16:20-16:40	360Vulcan	qemu-kvm + Ubu...
Succeeded	16:40-17:40	NoTrace Sec	D-Link DIR-878
Failed	16:40-17:40	CARS	D-Link DIR-878
Gave Up	---	0x34567a61	D-Link DIR-878
Failed	16:40-17:40	Tianjun Team	D-Link DIR-878

11-17 DAY 2

Status	Time	Team	Target
Gave Up	---	CARS	Ubuntu 19.10/Cen...
Succeeded	09:20-10:00	ddd Team	Adobe PDF Reader
Succeeded	09:20-10:00	360Vulcan	Adobe PDF Reader
Gave Up	---	Huashui Team	Windows Server 2...
Gave Up	---	CC6900	Windows Server 2...
Gave Up	---	Hillstone Neuron	Windows Server 2...
Gave Up	---	360Vulcan	Windows Server 2...
Failed	11:20-12:20	Securicar	VMware Workstati...
Gave Up	---	ddd Team	VMware Workstati...
Succeeded	11:20-12:20	360Vulcan	VMware Workstati...
Succeeded	13:00-14:40	ddd Team	D-Link DIR-878
Succeeded	13:00-14:40	360 InfoSec	D-Link DIR-878
Succeeded	13:00-14:40	360 Chengdu Sec...	D-Link DIR-878
Gave Up	---	360Vulcan	D-Link DIR-878
Succeeded	13:00-14:40	SISLAB PWN	D-Link DIR-878
Gave Up	---	360Vulcan	iPhone 11 Pro + iO...

Project Zero

News and updates from the Project Zero team at Google

Thursday, August 29, 2019

A very deep dive into iOS Exploit chains found in the wild

Posted by Ian Beer, Project Zero

COMPUTING

How China turned a prize-winning iPhone hack against the Uyghurs

An attack that targeted Apple devices was used to spy on China's Muslim minority—and US officials claim it was developed at the country's top hacking competition.

By Patrick Howell O'Neill May 6, 2021

Didi Global bows to Chinese regulatory pressure, will delist from NYSE

JULIE ZHU AND KANE WU
HONG KONG
REUTERS
PUBLISHED DECEMBER 3, 2021

This article was published more than 6 months ago. Some information may no longer be current.

The Didi Global headquarters, in Beijing, on July 5.
TINGSHU WANG/REUTERS

The strange case of Alibaba's Jack Ma and his three-month vanishing act

Jack Ma's attack on the caution of China's business regulators was perceived as a direct challenge to the authority of the country's vice-president. Photograph: Aly Song/Reuters

TECH GIANTS ARE GIVING CHINA A VITAL EDGE IN ESPIONAGE

U.S. officials say private Chinese firms have been enlisted to process stolen data for their country's spy agencies.

DECEMBER 23, 2020, 6:00 AM

By Zach Dorfman

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent me
affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

打开新浪新闻 发现更多精彩

新浪科技 > 互联网

周鸿祎:马云提新零售 我想了几个月想到了“大安全”

新浪科技
2017.09.12 14:01
+ 关注

周鸿祎接受采访

新浪科技 韩大鹏

“不要逞一时匹夫之勇，得了第一名，so what，虚！”

In an unexpected statement, billionaire founder and CEO of Chinese cybersecurity giant Qihoo 360, one of the leading tech companies in China, publicly criticized Chinese citizens who went overseas to participate in hacking competitions. In an interview with the Sina news site, Zhou Hongyi said that good performances at such events represented only “imaginary” success. Zhou warned that many hackers in his country were banned from participating in these contests or displaying minor hacks so that the Chinese government could have control.

GOVERNMENT

China's government is keeping its security researchers from attending conferences

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Ministry of Industry and Information Technology Network Information Office Security Department
Notice on Issuing the Provisions on the Management of Security Vulnerabilities of Network Products

Ministry of Industry and Information Technology Network Security [2021] No. 66

All provinces, autonomous regions, municipalities directly under the Central Government and Xinjiang Production and Construction Corps in charge of industry and information technology, public security departments (bureaus), and Cyberspace Administration of China, and communications administrations of all provinces, autonomous regions and municipalities directly under the Central Government:

The "Regulations on the Management of Security Vulnerabilities of Network Products" are hereby issued and will come into force on September 1, 2021.

Ministry of Industry and Information Technology

Cyberspace Administration of China

Ministry of Public Security

July 12, 2021

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

(2) The relevant vulnerability information shall be submitted to the network security threat and vulnerability information sharing platform of the Ministry of Industry and Information Technology within 2 days. The submitted content shall include the product name, model, version, and technical characteristics, harm , and scope of influence of the vulnerability that have network product security vulnerabilities.

Article 6 Relevant organizations and individuals are encouraged to notify network product providers of security vulnerabilities in their products.

Article 14 Whoever collects and releases network product security vulnerability information in violation of these regulations shall be dealt with in accordance with the law by the Ministry of Industry and Information Technology and the Ministry of Public Security in accordance with their respective duties; punished in accordance with this provision.

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

China's Ministry of Industry and Information Technology suspends Alibaba Cloud partnership over security lapse

Says it was not informed about a significant vulnerability

December 22, 2021 By: Sebastian Moss Be the first to comment

China's Ministry of Industry and Information Technology has suspended an information-sharing partnership with Alibaba's cloud division.

The government regulator claimed that Alibaba failed to promptly report and address a cybersecurity vulnerability.

An Alibaba cloud security engineer was the first person to find and report a significant cybersecurity loophole.
Photo: Qilai Shen/Bloomberg via Getty Images

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Wetgeving

Artikel 7 van de nationale inlichtingenwet van China stelt: "Elke organisatie of burger moet het inlichtingenwerk van de staat ondersteunen, assisteren en eraan meewerken in overeenstemming met de wet, en alle kennis van het inlichtingenwerk van de staat geheimhouden.“

Artikel 28 van de Chinese cyberbeveiligingswet stelt: "Netwerkoperators bieden technische ondersteuning en assistentie aan […] veiligheidsorganen die de nationale veiligheid waarborgen en criminele activiteiten onderzoeken in overeenstemming met de wet."

Artikel 11 machtigt de Chinese inlichtingendiensten om informatie te verzamelen en te verwerken over alle activiteiten van "overzeese entiteiten of individuen" die de nationale veiligheid en belangen van China in gevaar brengen.

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

CHINA

SUBMISSION TO THE NPC STANDING COMMITTEE'S LEGISLATIVE AFFAIRS COMMISSION ON THE DRAFT "NATIONAL INTELLIGENCE LAW"

AMNESTY INTERNATIONAL

"vague and overbroad concepts of "national intelligence" and "national security" as used in this law"

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

POLITICS BUSINESS TECH CHINA HUAWEI VODAFONE » MORE TAGS

SHARE THIS:

FRIDAY, 21 MAY 2021 - 11:26

Huawei blocked from core 5G networks of major Dutch providers

Chinese technology company Huawei no longer supplies components to the core 5G networks of major Dutch telecom providers, FD reported. The decision is likely a result of several Dutch secret services finding the company to be the long arm of the Chinese government, potentially posing a threat to the national security of the Netherlands.

A report accusing Huawei of having once had "unlimited access" to phone calls made using one of the Netherlands' leading operators, KPN, has been published by a Dutch newspaper.

The report was compiled by the CapGemini consultancy in 2010 but never released.

Those affected would have included former Prime Minister Jan Peter Balkenende.

The Chinese technology giant has completely denied the allegations.

TECH POLICE MINISTRY OF DEFENSE DRONE DATA LEAK CYBER ESPIONAGE » MORE TAGS

SHARE THIS:

THURSDAY, 30 SEPTEMBER 2021 - 09:17

Dutch police using Chinese-made DJI drones the Defense Ministry rejected over security concerns: report

The Dutch police regularly use drones made by Chinese company Da Jiang Innovations (DJI), which the Ministry of Defense banned over serious concerns about data security. There are various indications that images and other data from the drones leak to the Chinese government, Trouw, De Groene Amsterdammer and EenVandaag reported based on an investigative report by Investico.

NOS Nieuws • Dinsdag 8 februari 2022, 12:00 •
Aangepast dinsdag 8 februari 2022, 14:34

Omstreden Chinese camera's hangen overal in Nederland, ook bij ministeries

Joost Schellevis en Thomas Spekschoor

In ruim vijftig gemeenten in Nederland hangen camera's van de Chinese merken Hikvision en Dahua, blijkt uit onderzoek van de NOS. De merken zijn populair maar controversieel: de camera's zijn goed en niet duur, maar er zijn zorgen over spionage en mensenrechtenschendingen door de fabrikanten.

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

China's Tsinghua University linked to cyber espionage, study claims

Targeting of Daimler, state of Alaska and Tibetan groups traced to college computer

'Kennis naar Chinees wapentuig'

Tientallen Chinese militairen actief op Nederlandse universiteiten: 'Zorgelijk'

20 mei 2022 16:14
Aangepast: 20 mei 2022 18:11

Chinese militaire wetenschappers werken op Nederlandse universiteiten

"Hoogwaardige Nederlandse kennis komt terecht in Chinees wapentuig en dat is zorgelijk." Deze duidelijke waarschuwing komt van directeur Jan Swillens van de Militaire Inlichtingendienst (MIVD).

CRIME | CHINA

Netherlands probes 'illegal' Chinese police stations

Premier Mark Rutte ontving in oktober premier Li Keqiang van de Volksrepubliek China. Beeld ANP

De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst (MIVD) slaat alarm om de uitdijende invloed van China. Die waarschuwing kan voor verdere druk zorgen op het kabinet, dat al maanden bezig is een China-strategie op te stellen.

Ruim 900 Nederlandse bedrijven in Chinese handen, ook ICT

Nederland belangrijke bestemming voor Chinese investeringen.

2

© CC0/Pixabay License

28 SEPTEMBER 2022

Chinese bedrijven of de Chinese staat hebben meerderheidsbelangen in 903 bedrijven in Nederland, waaronder ook ICT-ondernemingen. Dit blijkt uit een nieuw overzicht dat is samengesteld door RTL Nieuws en Follow the Money (FTM). Zorgen over afhankelijkheid, spionage of zelfs sabotage spelen hier mee.

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Food for thought ...and how KPMG can help

In hoeverre worden de volgende vragen al binnen uw organisatie gesteld?

- Is mijn organisatie als sector interessant voor nation states?
- Hoe blijven wij op de hoogte van activiteiten en –mogelijkheden van statelijke actoren met een offensief cyberprogramma?
- Hoe ga ik om met mobiele datadragers wanneer ik naar een land reis met een offensief cyberprogramma?
- Op welke manier kan buitenlandse inlichtingen- en cyberwetgeving voor mijn organisatie een risico vormen?
- Welk IP en/of bedrijf kritische afhankelijkheden heb ik te beschermen in de toeleveringsketen?
- Hoe ga ik om met insider threat? Hoe gaat mijn organisatie om met screening (en monitoring) van potentiële werknemers die gaan werken in de gevoeligste onderzoeksgebieden van mijn organisatie?

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG Cyber and privacy

Prevent	Improve	Detect	Respond
			
Strategy & governance	Transformation	Cyber defense	Cyber response
Aligned with client business priorities and compliance needs			
• Security assessment & certification • Cyber strategy / Target Operating model dev. • Chief Information Security Officer metric & reporting • Information governance & privacy • Third-party security risk management • Cyber Risk Management • Business continuity • Operational resilience	• Identity and access management • Security GRC • Security technology architecture & E2E integration • Program delivery & management • SAP Security • CRM Security • Data Loss Prevention • Capacity & capability development	• Technical assessments (incl. Red-teaming & AMS) • Cyber Threat Intelligence (CTI) • Security operations and monitoring • Security analytics	• Incident response, coordination and planning • Digital investigations & remediation • Forensics • Incident recovery support

Expert detachering I Project en programmangement I Advies en thought leadership I Awareness & training

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

For more information

Please contact:

Marcel van Kaam

Senior Manager KPMG Cyber
+31 6 2325 7205
vankaam.marcel@kpmg.nl

Justin Black

Senior Manager KPMG Cyber
+31 6 13017109
black.justin@kpmg.nl

© 2022 KPMG N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

© 2022 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

De naam KPMG en het logo zijn geregistreerde merken die onder licentie worden gebruikt door de zelfstandige ondernemingen die lid zijn van de wereldwijde KPMG organisatie.

De in dit document vervatte informatie is van algemene aard en is niet toegespitst op de specifieke omstandigheden van een bepaalde persoon of entiteit. Wij streven ernaar juiste en tijdige informatie te verstrekken. Wij kunnen echter geen garantie geven dat dergelijke informatie op de datum waarop zij wordt ontvangen nog juist is of in de toekomst blijft. Daarom adviseren wij u op grond van deze informatie geen beslissingen te nemen behoudens op grond van advies van deskundigen na een grondig onderzoek van de desbetreffende situatie.

Document Classification: KPMG Public