出國報告（出國類別：考察）

參與瑞士資安日活動出國報告書

服務機關：數位發展部資通安全署

姓名職稱：林郁智科長

派赴國家：瑞士

出國期間：113 年2月17日至23日

報告日期：113 年 5 月

摘 要

此次出國任務係考察第 5 屆瑞士資安日（SCSD）活動於 2024 年 2 月 20 日至 21 日於瑞士伯恩舉行。其中我國數位發展部唐鳳部長受邀以預錄方式發表演說，為唯一受邀的亞洲國家資安部長級官員，並以數位發展部部長名義發表演說。此外，資通安全署與會代表，在駐外管處同仁協助下，於展區設置臺灣形象館，透過影片、宣導品與現場解說向與會者展示臺灣資安及經貿實力。主辦單位 Dreamlab Technologies 公司為瑞士資安服務廠商，與瑞士政府有關機關共同舉辦瑞士資安日活動，分享相關網路安全等專業領平臺，結合各國專家學者一同商討致力提升網路安全性。

本次為第 5 屆瑞士資安日，活動主要來自全球的產、官、學界人士超過 2,200 人參與，共同探討網路安全相關議題，包含網路犯罪等，為瞭解國際網路資通訊安全議題及網路威脅情資新知、協力共創安全的網路環境，資安署派員考察資安日活動，以掌握最新網路資通安全樣態及因應之道。

目 次

壹、目的

瑞士資安日 Swiss Cyber Security Days（SCSD）是瑞士及歐洲地區，就網路安全領域具有領導地位的論壇。每年聚集自世界各地的資安領域專家，致力討論網路安全相關議題。藉由主題論壇、專業技術論壇及廠商參展活動區，進行國際資安政策、技術及產品服務趨勢交流，論壇中所討論的議題，結合技術、研究、政治、商業等面向，不僅對於當前網路威脅進行剖析，也提供各國增進網路安全維護方案的創新想法，我國數位發展部資通安全署也派員實際與會，就相關議題跟與政府代表及學者，分享我國資安領域的努力與成果，也為我國資安國際合作拓展能量。

數位發展部唐鳳部長本次受邀於 2 月 20 日下午針對網路安全與數位主權(Cyber Security & Digital Sovereignty)發表預錄演講，為唯一受邀的亞洲國家資安部長級官員，並以數位發展部部長名義發表演說。我國亦受邀在公共展區亦設置臺灣形象館，透過影片、宣導品與現場解說向與會者展示臺灣資安及經貿實力。是以本次公務出國目的除考察資安日活動外，亦確認唐部長發表預錄演說相關之行政事宜。

一、 **活動合作商**

Dreamlab Technologies 公司為主辦方，主要合作方為瑞士伯恩經濟發展局(官方)及其他知名資安相關民間企業。

二、 **活動模式**

活動設計分為三個區塊，主要論壇區、技術論壇區以及廠商展示區。主要論壇區及技術論壇區是以主題式演講方式進行或是以圓桌方式進行討論；廠商展示區，世界各國資安相關廠商擺設展示位，進行產品介紹、宣傳等三個區塊。

貳、考察經過

一、 **日期：**2024 年 2 月 20 日(星期二)至 21 日(星期三)

二、 **地點：**瑞士伯恩

三、參與場次表：

日期	重點參加場次
2 月 20 日	開幕式
	Findings and consequences for national cyber security agendas
2 月 21 日	Cybercrime as a threat to Switzerland
	臺灣形象館展場

四、活動重點摘要

(一) 開幕式

1.致詞者：

(1)National Councillor Doris Fiala[1] (前自民黨國會議員)

[1] 圖片及說明來自官網 https://scsd.ch/en/conference_talks/243

Doris Fiala

Former FDP National Councillor President of Swiss Cyber Security Days
Member of the Board of Directors of Opernhaus Zürich AG

Doris Fiala was a member of the Swiss FDP National Council from 2007 to 2023 and President of FDP Women Switzerland for three years. She has been President of the Swiss Cyber Security Days since 2019. She is also a member of the Board of Directors of Zurich Opera House.

(2) Alec von Graffenried[2](伯恩市長)

Alec von Graffenried

Major of Bern

Alec von Graffenried is a Swiss politician and has been Mayor of Bern since 2017. After completing his law degree at the University of Bern, he worked as an advocate, first for the Canton of Bern and then in his own law firm. He also served as governor of the administrative district of Bern and was responsible as a director of Losinger Marazzi AG.

[2] 圖片及說明來自官網 https://scsd.ch/en/conference_talks/243

(3)Nicolas Mayencourt[3](Dreamlab Technologies 全球執行長)

Nicolas Mayencourt

Global CEO Dreamlab Technologies and Program Director SCSD

Nicolas Mayencourt is the founder and Global CEO of Dreamlab Technologies, a Swiss IT security company that has been hacking the computer systems of companies, states and authorities for over 25 years - legally and at their request - in order to subsequently develop suitable security concepts and solutions. As programme director of the Swiss Cyber Security Days, Mayencourt is also responsible for putting together the two-day programme.

2.重點摘要：

(1) 全球各方面威脅不斷:

本世紀的威脅包括氣候變遷、環境變化、核子威脅、流行病、政治混亂和極端主義以及接下來的生活人工智慧。 網路攻擊在 2020 年 IQ 國際電信單位排名中，瑞士排第 42 名。

(2) 建立安全網路空間:

對於民主影響非常重要，尤其是承擔資訊的危險。網路空間可以儲存公眾意見並影響決策，對於媒體資訊來源進行確認、批判性策略，強化媒體素養就顯得非常重要。網路犯罪透過控制宣傳和操縱，必須採取立場來應對這些威脅。事實查核和國際合作變得越來越重要。網路安全可以保護線上平台和 IT 系統免受攻擊，從而有助於遏止虛假資訊的傳播。

(3) 政府、科技公司和民間社會須共同努力負責:

社群媒體平臺上實施安全機制，以確保使用者帳戶和資訊的完整性。 瑞士資安日為交流網路安全領域的知識經驗和最佳實踐提供了平台。

[3]圖片及說明來自瑞士資安日官網 https://scsd.ch/en/conference_talks/243

(4) 網路釣魚和勒索軟體:

攻擊不僅對受影響的人來說風險外，歐盟估計，網路犯罪每年對企業造成的損失達數 10 億歐元。一項網路安全研究預測，全球網路犯罪造成的損失將上升至超過 19 兆美元。

(二) Cyber Security & Digital Sovereignty

1.講者：Christian-Marc Lifländer [4](北約網路防禦機構負責人)

Christian-Marc Lifländer

Head of NATO Cyber Defense Section

As Senior Cyber Policy Officer on NATO's International Staff, Christian-Marc Lifländer is responsible for the development and implementation of cyber defense policy across NATO. Previously, he worked as an advisor in the Estonian Ministry of Defense, as Director of Policy Planning and Advisor to the Minister of Defense. Lifländer has received several awards from the Estonian Ministry of Defense for his work.

2.重點摘要：

北約已將網路空間定義並承認為戰爭領域。因此，網路防禦是集體防禦不可分割的一部分。可以明確知道，沒有合作夥伴，就無法防範網路攻擊。

(1) 網路空間是全球戰略競爭關鍵舞臺

網路空間和新興科技成為全球戰略競爭的核心關鍵舞台。面臨來自戰略競爭對手的各種網路攻擊、假訊息傳播等威脅，對民主體制、國民

[4] 圖片及說明來自瑞士資安日官網 https://scsd.ch/en/conference_talks/1226

安全以及全球經濟體系都造成了嚴重衝擊，對此應有清晰的認知並做好準備。

(2) 新興科技對網路防禦的影響:

人工智能、量子計算等新興科技已改變網路空間的特性。這些科技可為民眾使用，也可能被國家用於軍事用途。民主國家無法掌控這些關鍵新興科技技術，很可能會被獨裁國家所主導，這將對網路安全、個人隱私以及經濟繁榮造成嚴重威脅。NATO 對此也採取相應措施，例如加速研發及創新，以保持科技技術優勢。

(3) 加強公私部門參與，建立國際緊密合作:

面對網路安全威脅，公私部門必須緊密聯繫，並建立長期合作制度。需要政府、民間企業、國際組織等各方共同努力，共同應對戰略競爭對手的威脅，維護網路空間的自由、開放，共同推進和平與安全，並堅守民主規範和價值觀。

(三) Cyber Security & Digital Sovereignty

1.講者：Tomáš Minárik[5] (捷克國家資安暨資訊署負責人)

Tomáš Minárik

Head of the International Organisations and Law Department at NÚKIB

National Cyber and Information Security Agency NÚKIB Tomáš Minárik has headed the International Organisations and Law Department at the Czech National Agency for Cyber and Information Security (NÚKIB) since 2019. Prior to that, he worked as a researcher in the legal department of NATO, focusing on legal aspects of cyberspace operations, activities of international organisations in cyberspace and cyber defence exercises. Previously, he worked as a legal advisor for the Czech Ministry of Defence.

[5]圖片及說明來自瑞士資安日官網 https://scsd.ch/en/conference_talks/1226

2.重點摘要：

(1) 捷克自 2018 年以來在監管供應鏈安全方面的經驗：

5G 業務發展包括遠程手術，無人駕駛電動車等，當時為了推展 5G 業務，採用中國相關設備，但是設備經過評估有網路安全風險，當時政府也採取了相關措施，後續並擴大到供應鏈範圍，供應商負有法律義務確保資訊安全並製定供應鏈安全機制的流程，政府全面支持經風險評估之供應商，以提供良好網路安全及網路防禦。

(2) 全球戰略情勢與國防安全支出的必要性:

在網路安全和網路防禦方面， 擁有良好的防護能力非常重要。2014 年到 2022 年包括氣候變遷、特定國家的有意活動，造成無法預測重大變化。俄烏戰爭下，俄羅斯可以將 GDP40%用於戰爭，實體攻擊與網路攻擊，所以國家最優先的支出是國防安全的訓練並增強韌性。

(3) 網路安全的國際合作：

除了國家層面外，北約「卓越聯合網路防禦中心」設置在愛沙尼亞，主要是執行網路防禦研究、策略及法律諮詢建議，由跨國及跨產業專家組成，以支援北約及其成員國。中心參與者約 40 個。關注聯合國國際網路法層面，圍繞全球基礎設施，進行網路能力建置，並關注幾個地區的影響。

(4) 選定新興性技術建立全國橫向工作小組

技術合併，設立機構負責處理機密資訊的資訊系統安全。另外強化與衛星服務安全的合作對象，成立橫向工作小組（5 個領域、技術），包含國家量子戰略、通訊基礎設施事項。

(四) Cyber Security & Digital Sovereignty

1.講者：Audrey Tang[6]（臺灣數位發展部部長）

Audrey Tang

Minister of Digital Affairs, Taiwan

She was able to program at the age of eight, is considered a first-class hacker, is the first transgender minister worldwide and is committed to digital democracy. Today, she is considered the first Taiwanese free software programmer as well as the first Minister of Digital Affairs of the Republic of China. Audrey Tang is known for the invention and main development of the PAR tool and the initiator and leader of the Pugs project. She has been involved in over 100 Perl projects and introduced smoke tests and digital signatures in CPAN.

2.重點摘要：

(1) 臺灣數位韌性:

臺灣數位發展部負責強化數位韌性的使命，包含事件應變韌性、產業韌性和社會韌性等 3 個層面。事件應變韌性是有效處理各種危機的方法，例如網路駭客攻擊、地震颱風災害及其他自然災害。資安防護僅靠單一國家無法有效防護，需仰賴國際合作。例如，數位發展部資通安全署積極建立國內、外聯防機制、多元合作關係與資安事件、情資分享管道，推動與各國合作，例如參與北約網路安全會議(CyCon)、2023 年舉辦跨國網路攻防演練(CODE)及「前瞻資安探索會議」(ACE)，透過交流強化我國關鍵基礎設施之資安防護與通報應變之能力，有效因應不斷更新的資安威脅，強化資安防護。

[6] 圖片及說明來自瑞士資安日官網 https://scsd.ch/en/conference_talks/1226

(2) 臺灣的首要任務是加強網路安全防護:

臺灣面臨的資安威脅，主要是侵入性攻擊，超過百分之 40%，例如透過應用程式、未獲授權取得使用者權限等。為此，政府機關網路採用零信任架構。

(3) AI 挑戰與創新:

在臺灣，AI 包含兩大主要層面：源頭合作和社會檢視。為了鼓勵大眾參與 AI 發展過程，以公眾智慧挑戰 AI，數位發展部在 2023 年正式成為國際非政府組織「集體智慧計畫」(Collective Intelligence Project， CIP)合作成員，結合 OpenAI、Anthropic 等業界發起對準(Alignment Assemblies)專案。數位發展部從人才、技術、產業及驗證等四大面向推動產業 AI 化，積極加入國際組織，發展與國際接軌的 AI 規範及標準，提升臺灣 AI 在國際的影響力。

(五) Cybercrime as a threat to Switzerland

1.講者：Prof. Dr. Joël Mesot(蘇黎世聯邦理工學院校長)

Prof. Dr. Joël Mesot

Präsident der ETH Zürich

The Swiss physicist Joël François Mesot is a full professor at the Swiss Federal Institute of Technology (ETH) in Zurich and has been the President of ETH Zurich since 2018, having been elected by the Federal Council. He previously designed and realised the neutron time-of-flight spectrometer FOCUS at the Paul Scherrer Institute PSI before moving to the University of Illinois, Chicago, where he conducted research into quantum materials on synchrotons. He then returned to PSI, where he headed the Laboratory for Neutron Scattering. He was later awarded a titular professorship at ETH Zurich and a dual professorship in Zurich and at the EPF in Lausanne.

2.重點摘要：

網路犯罪對瑞士而言是一個威脅，必須透過研究及創新才能應對。網路攻擊對公共部門和民間企業都構成威脅。大學也不例外，必須對來自網路空間的威脅做出適當的反應，並保護大學研究的寶貴數據。可以了解蘇黎世聯邦理工學院如何幫助瑞士增強資安韌性。

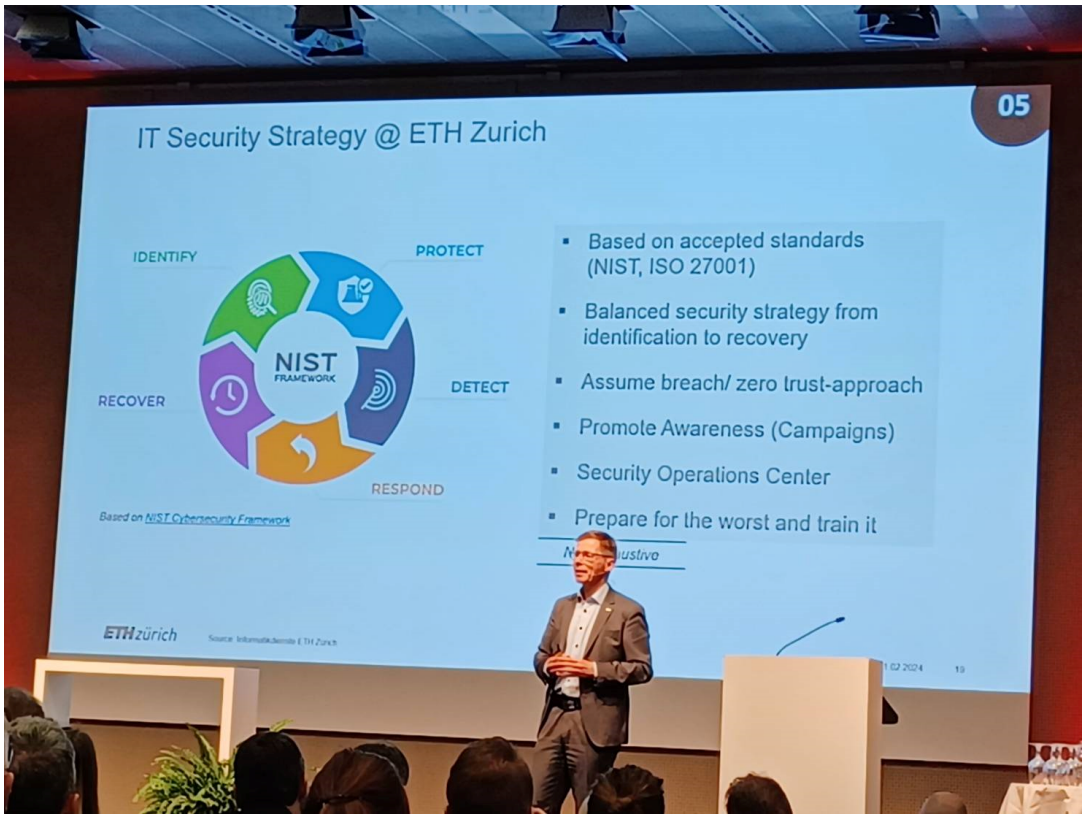
(1) 說明大學也是收到資安攻擊的對象，而且攻擊的數量與年俱增。

(2) 介紹瑞士蘇黎世聯邦理工學院在資安領域範圍、相關機構等，包含教授、學生、資金近 10 年來成長率。

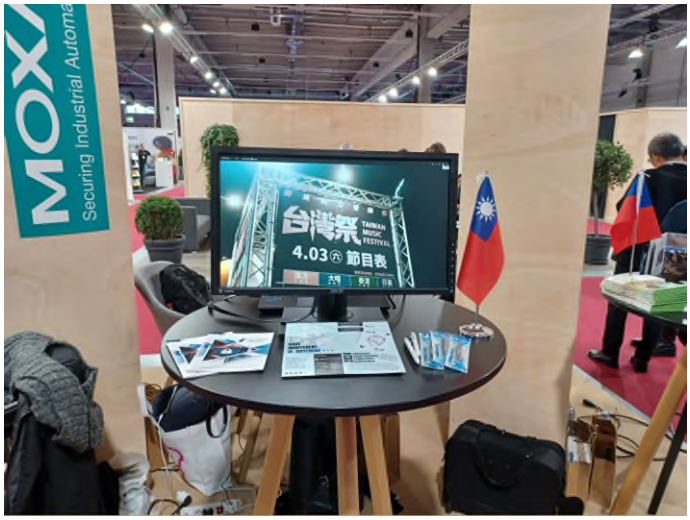
(3) 面對全球化挑戰，有五個層面，健康與福祉、責任數位轉型、環境與資源、社會對話、基本原則等，有三個與網路安全息息相關。

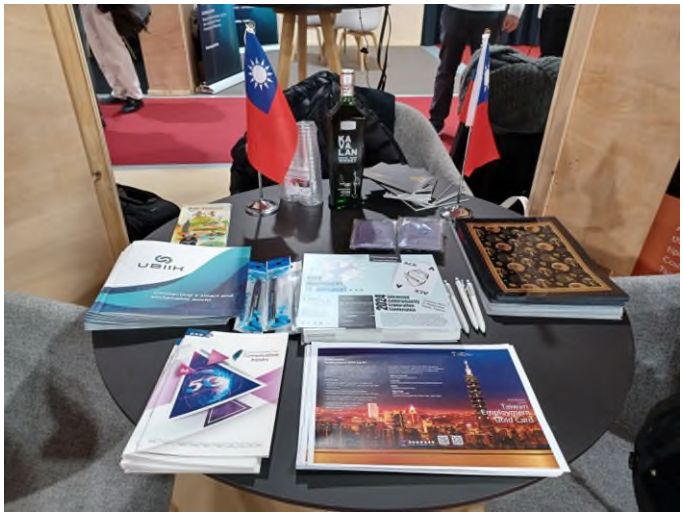
(4) 蘇黎世聯邦理工學院對於資安領域人才之培養、設有資訊安全及隱私中心，增強數位關鍵技術能力。

(5) 蘇黎世聯邦理工學院的 IT 安全策略，認證、保護、偵測、回應及復原。



（六）臺灣形象館


Securing Industrial Automa
台灣祭
TAIWAN MUSIC FESTIVAL
4.03㈥節目表




Taiwan
THE HEART OF ASIA
Fascinating
TAIWAN
Taiwan
THE HEART OF ASIA
MOXA
Securing Industrial Automation
illumio
Segment to
stop the spre
of breaches

1. 場地:

本次我國受邀在公開展示區設置臺灣形象館,現場廠商有中華航空、肆零肆、金車等企業進駐,趨勢科技亦自行設攤。現場以持續撥放影片方式推廣臺灣,包含數位發展部 2023 年舉辦之 CODE 及 ACE 活動影片,現場亦備有文宣,宣傳今年度 ACE 活動,邀請與會者共襄盛舉。現場並有外館人員積極推銷臺灣,包含推廣臺灣葛瑪蘭威士忌、臺灣觀光、臺灣資安活動等,並主動邀請其他外國廠商、人員至臺灣形象館參觀,強力行銷臺灣。

2. 最常被問到的問題,臺灣平均每日受到的資安攻擊有多少次?如何抵禦這些攻擊?臺灣的資安組織為何?面對周邊國家資安威脅,有什麼解決方案等問題。

參、心得與建議事項

1.瑞士資安日活動:

瑞士資安日活動分為三個區域，建議可依區域性質由不同機關人員出席。

(1) 主要論壇:

多為政策性議題，如國際資安趨勢、國際現狀，可聚焦於國際合作，且與會人士亦有其他國家或國際組織代表出席參與，建議一定層級之長官人員出席，進而參與討論，適時提供臺灣相關資安政策或作為。本次即由數位發展部唐鳳部長，以部長名義預錄發表演說，現場反應熱烈。如實際出席會議，勢必為現場焦點，可有效行銷臺灣。

(2) 技術論壇:

多為技術專業領域討論，建議由具一定資安專業技術人員出席，可實質參與討論並獲取國際資安新知、新技術等。

(3) 展覽區:

此區多為資安廠商參展，來年如仍獲邀擺設臺灣形象館，建議經貿及資安產業主管機關派員，現場為推銷商品，詢問臺灣資安現狀及有無需要相關商品或服務，或有欲開拓我國市場者，可進行行銷及宣傳。

(4) 其他:

瑞士伯恩為德語區，故瑞士資安日活動相關場次超過 5 成以德語進行演說，雖有英語同步口譯，但理解上相對困難。後續如繼續參加此活動，建議併予考量。另派員應給予出國人員適當時間準備行程、整備資料及資訊。

2. 政府在瑞士資安日活動可參與之角色

(1) 我國囿於國際情勢、兩岸關係及地緣政治等因素，在參與官方及非官方國際組織均有一定難度。本活動主辦方為民間企業，但共同舉辦方為瑞士官方機構，活動參與者亦有其他國家或國際組織之前、後任官員(如烏克蘭、捷克、北大西洋公約組織、歐盟)、國際資安專家學者等，潛在參與者之官方色彩濃厚。且觀察活動受邀請者大多為民主制度國家之

產、官、學界代表，建議政府可在此多著墨。藉由此平台行銷臺灣、介紹我國資安組織、現況、國家資安政策、資安威脅趨勢之因應方案，並可把握機會尋求參與國際組織進行國際合作，建立國際聯防機制，組成國際資安聯盟陣線等，強化成員間之數位韌性，進行資安情資分享。

(2) 即時更新國際資安趨勢、預判資安威脅，進而提升國家資安防護。藉由活動參與，掌握國際資安關注議題，資安領域新興科技，並可藉由參考其他與臺灣相類國家之政策面、技術面、法制面，滾動式調整國內資安防護政策、扶植資安產業、適時引進新興資安防護技術等。

(3) 在網路已經融入日常生活之數位時代，人們日常之食、衣、住、行，各種經濟活動透過數位方式之應用需求，以 app、電子支付工具已成為不可或缺的一環。隨之而來是不肖人士藉由惡意軟體竊取用戶個人資料勒索贖金、網路詐騙事件頻傳，加上加密貨幣之盛行，阻斷相關金流，讓檢、警、調在網路犯罪相關案件偵辦上更趨困難。我國今年 4 月 30 日立法院三讀通過之電子簽章法，除可與國際接軌外，電商平臺可向網路賣家要求數位簽章，以類似實名制確認賣家身分，防止不肖業者欺詐的行為，可以預見在未來能有效降低網路犯罪發生率。

附錄：

一、唐部長發表預錄演講

二、場地外觀


WILLKOMMEN
BIENVENUE
WELCOME


SWISS CYBER SECURITY DAYS
LET'S GET DIGITAL!
SCAN ME!
SHAPING CYBER RESILIENCE
SWISS CYBER SECURITY DAYS
LET'S GET DIGITAL!
SCAN ME!
SHAPING CYBER RESILIENCE

三、場內


SHAPING CYBER
RESILIENCE


SWISS CYBER SECURITY DAYS
LET'S GET DIGITAL!
Browse through exhibitors and their products
Discover the diverse program
Scan exhibitors during your visit
Set yourself favorites
Find your way around the Swiss Cyber Security Days area
SCAN ME !
Event Guide
PARTNERS
DIAMOND PARTNER
DREAMLAB TECHNOLOGIES
PREMIUM PARTNER
Standortförderung Kanton Bern
ELITE PARTNER
CISCO
CLOUDFLARE
CROWDSTRIKE
DELL
DIGITAL REALTY
ELCASecurity
mimecast
paloalto
SailPoint
SOPHOS
sosafe
SUSE
swisscom
TREND