資安長2021年新職責：從風險減緩到業務促進

從供應鏈駭客攻擊到 5G 部署，現有及新的挑戰將繼續考驗安全團隊擴大的角色。

文／Rick Grinnell 譯／PL

2020年，資安長（CISO）面臨許多挑戰，其中最重要的挑戰是COVID-19及為此而從現場轉為遠端工作的大規模遷徙作業。也許這是是第一次，企業領導人了解到安全團隊對確保公司運營及平順運營有多麼重要，這因此使得2020年成了資安長及網路安全團隊從幕後走到幕前，協助提升組織生產力的一年。

> **在家工作的員工不是唯一使用家裡 WiFi 的人，資安長在考慮公司網路安全時，需要納入一個家庭裡每個人的行為。**

時至2021年，資安長及他們的安全團隊可望繼續展現其角色從減緩風險、到提升投資報酬的重要性——因為他們必須解決供應鏈駭客攻擊、勒索軟體、在家工作(WFH)、5G推出等諸多挑戰。

供應鏈駭客的影響

當2020年來到尾聲（這是怎樣的一年啊！），迎向2021年的資安長試圖了解SolarWinds駭客攻擊事件及它會如何影響他們自己的組織。正如CNET的解釋，「對駭客而言，要完成一起供應鏈攻擊是一件大事，因為它要將惡意軟體打包在受信任的軟體中。」政府機構是我們知道的第一個目標，但是看來也會連帶讓其它數十家公司受到影響。那些受影響的人將投入接下來的幾週、幾個月的時間，找出他們的系統如何能在近一年的時間裡無法偵測到某人，並找出損害。

勒索軟體

勒索軟體將持續成為2021年的問題，資安長可以預期看到威脅者在他們的攻擊中變得更具創意。勒索服務(ransomware-as-a-Service, RaaS)是一種快速又簡便能讓駭客賺點錢的方法——RaaS構建器的成本約為40美元，社交媒體上可以找到如何進行攻擊的視頻。

國家也會發起勒索軟體的攻擊，目標是對關鍵基礎設施採多階段攻擊。它們一開始先採暴力破解方法獲取管理密碼，然後建立後門進入網路。進入內部之後，便會將惡意軟體佈署其中以便找出端點，一旦完成，勒索軟體便會被啟動。我們看到2020年曾發生幾起知名醫療機構成為這類攻擊的受害者，而2021年將有朝此錯誤方向持續發展的趨勢。

遠端勞動力

員工2021年無法順利返回辦公室。在家工作將一直持續到疫苗全面推出，甚至更長的時間為止。這意味著，現在併用的任何網路安全系統都必須維持有效，或針對處於家庭／辦公室工作混合模式中的員工進行修改。網路罪犯了解這點，因此他們會透過網路釣魚及其它針對性攻擊將遠端工作者視為攻擊目標。資安長可以預見圍繞著COVID-19疫苗的網路釣魚活動，像是「提議」如何超前你的鄰居列在疫苗候補名單上。

網路釣魚不會是唯一的問題。遠端工作者會繼續使用自攜設備(BYOD)，包括做為節慶禮物收到的新設備，而那很可能會引發網路安全的問題。如果公司尚未制定遠程工作期間監控員工自攜設備的計畫，那麼資安長可能會想要將這納入他們2021年的計畫中。

來自家庭內部的威脅

在探討來自家庭內部的威脅時，這些都不是來自員工或合作廠商的威脅，而是來自公司勞動力實際家庭的內部威脅。員工不是唯一使用家裡WiFi的人，資安長在考慮公司網路安全時，需要納入一個家庭裡每個人的行為。

在假期過後，各個家庭都忙於裝置新的門鈴攝影鏡頭及使用雲端的語音服務（像是Alexa），而所有這些物聯網設備都會增加額外的風險。又或者，孩子們也許會獲得Microsoft或SONY的最新遊戲機，或訂閱他們最喜歡的線上遊戲。2020年12月，託管諸如Dota等一些最受歡迎的遊戲的Steam便發生一起遊戲客戶端存在嚴重漏洞，導致駭客可以透過這些漏洞接管與該遊戲客戶端連接的任何電腦。

遠端存取及遭竊的身份憑證

遠端存取的需求可能導致憑證被盜。如果惡意方能夠取得你的員工的身份憑證（可能透過上述前三項威脅趨勢），那麼惡意方就可以存取該員工所做的任何事物。資安長也不能仰賴「虛擬私人網路」(VPN)確保網路存取的安全。

我們就以去年夏天的Twitter駭客為例吧。這名十幾歲的駭客能從Twitter員工那裡竊取VPN憑證，並利用該資訊存取歸屬世界上一些最知名人士的Twitter帳戶的憑證，然後讓這些人士的追隨者相信「迅速致富」這類的詐騙主張。該名駭客從這場騙局中獲得超過10萬美元的利潤，而Twitter顯示透過一個人的憑證存取該網路是多麼容易的事。

圍繞著「隨處工作」生產力的安全議題

已從在地網路轉為雲端網路的組織讓遠端工作變得可行，並允許工作人員保持生產力。不過，維持雲端安全將會成為資安長的挑戰。安全團隊需要仔細檢視身份及存取管理系統，以防止憑證遭盜、改善雲端環境中的監控及保護雲端的專屬與敏感資料。

5G的推出

2021年會是5G真正產生影響的一年嗎？或許吧，但是無論如何，資安長及其安全團隊都需要為5G衍生的安全挑戰做好準備。我們尚不清楚公司或威脅者會如何利用5G，但是我們確實知道，憑藉更快的連結及更低的延遲等優勢，未來將有更多設備同時使用5G的功能。組織需要做好準備保護愈來愈多的這些新端點，尤其是當它們持續管理遠端勞動力的安全性時。

2021年的多數安全將必須圍繞著預期很大程度是遠端勞動力打轉，但是許多安全問題——例如勒索軟體、憑證遭盜及雲端威脅——仍將是長期議題。資安長及其團隊愈能減輕圍繞這些威脅點的風險，便有愈多的事業運營不會受到干擾，從而再次證明安全團隊對領導階層的投報價值。