Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Ufficio federale della cibersicurezza UFCS

Misure per la ciber-resilienza nel contesto di grandi manifestazioni e conferenze internazionali

Le grandi manifestazioni e le conferenze internazionali possono condizionare la situazione di minaccia informatica. È altamente probabile che simili eventi siano utilizzati come punto di partenza per ciberattacchi o che i partecipanti e le loro organizzazioni siano direttamente presi di mira da attacchi informatici. I moventi e gli obiettivi degli autori possono variare, ma le misure di protezione di base non differiscono da quelle da adottare nel contesto di una situazione normale. Se tali misure sono effettivamente applicate è possibile evitare numerosi potenziali ciberincidenti.

In questa sede è fornita una breve panoramica delle misure di protezione di base raccomandate alle organizzazioni che partecipano a grandi manifestazioni e a conferenze internazionali. Molte raccomandazioni sono già note ai più da anni e sono ormai considerate come parte integrante delle *common best practices*. L'Ufficio della cibersicurezza (UFCS) raccomanda di applicare tali misure indipendentemente dall'attuale situazione di minaccia informatica e di notificare le attività sospette all'UFCS mediante il modulo di segnalazione[1].

Il presente documento non descrive le esigenze di protezione particolari delle organizzazioni coinvolte. Oltre alle misure menzionate in questa sede le organizzazioni devono considerare anche le minacce specifiche all'impiego e le conseguenti esigenze di protezione.

Misure prioritarie:

Le seguenti misure sono particolarmente efficaci per ridurre al minimo i ciber-rischi e aumentare la ciber-resilienza:

- **Protezione degli accessi da remoto**
  Tutti gli accessi da remoto quali VPN, RDP, Citrix, ecc. e tutti gli altri accessi alle risorse interne (ad es. webmail, SharePoint ecc.) devono essere imperativamente e costantemente protetti con l'autenticazione a due fattori (2FA) o con una chiave di accesso. Ciò vale anche per gli accessi da parte di fornitori, partner contrattuali ecc.
- **Gestione degli aggiornamenti («patch») e del ciclo di vita**
  Gli aggiornamenti di sicurezza devono essere installati regolarmente e tempestivamente su tutti i sistemi. Gli aggiornamenti che risolvono vulnerabilità di sicurezza critiche in sistemi accessibili via Internet devono essere effettuati entro 24 ore. I software e i sistemi non più supportati dal produttore («end of life», EOL) devono essere disinstallati o trasferiti in una zona di rete separata e protetta.
- **Backup offline**
  Effettuate regolarmente delle copie di sicurezza («backup») dei vostri dati secondo uno schema di rotazione (quotidiano, settimanale, mensile; min. due rotazioni). Dopo aver effettuato il backup ricordatevi di scollegare fisicamente il supporto che contiene la copia di sicurezza dal computer (e quindi dalla rete) e conservatelo in maniera sicura oppure utilizzate supporti di memorizzazione WORM.

[1] https://www.report.ncsc.admin.ch/it/

Ulteriori raccomandazioni per la protezione di base:

Le misure summenzionate riducono notevolmente i ciber-rischi. Si raccomanda tuttavia di rafforzare la protezione di base, nel limite del possibile, almeno con le seguenti misure supplementari:

- **Comunicare i dati di contatto dei possibili interlocutori in caso di eventi in materia di sicurezza**
  Comunicare i dati di contatto dei possibili interlocutori in caso di eventi in materia di sicurezza può risultare molto utile. Può per esempio consentire all'UFCS o alle autorità di perseguimento penale di stabilire rapidamente i contatti necessari in caso di allerta. Si raccomanda di utilizzare a tal fine lo standard «security.txt»[2].
- **Mantenere aggiornato il *business continuity management***
  È opportuno esaminare in che modo i processi chiave dell'attività commerciale dipendono dalle componenti IT e come la creazione di valore possa proseguire, almeno in parte, in caso di evento. Va inoltre verificato lo stato di aggiornamento delle procedure di emergenza e di crisi. Come minimo, deve essere chiaro chi informa chi e chi può prendere quali decisioni.
- **Impiegare una protezione dagli attacchi DDoS**
  Le applicazioni web, le piattaforme o i sistemi esposti a rischi in Internet e indispensabili per le attività commerciali vanno protetti dagli attacchi DDoS mediante una soluzione anti-DDoS interna o con il ricorso a un fornitore esterno di soluzioni anti-DDoS. Informatevi sulle possibili soluzioni presso il vostro provider di servizi Internet o presso il vostro provider di servizi di hosting.
- **Impiegare uno strumento di EDR/XDR per l'individuazione di anomalie**
  Per individuare e bloccare le attività sospette, impiegate uno strumento di EDR/XDR («endpoint detection and response») o di XDR («eXtended detection and response») su ogni client e server.
- **Limitare l'accesso ai sistemi esposti a rischi**
  Verificate l'accesso a sistemi, applicazioni e piattaforme esposti a rischi in Internet e limitate per quanto possibile i relativi accessi. A tal fine si può ricorrere ad esempio al blocco geografico («geo-blocking») o a una *allow list* per determinati indirizzi IP o per determinate reti IP («whitelisting»).
- **Verificare i file di log determinanti per la sicurezza**
  Verificate regolarmente e a ritmi ravvicinati le eventuali attività sospette dei file di log determinanti per la sicurezza, quali ad esempio i file di log dei software antivirus, degli strumenti di EDR/XDR, delle infrastrutture web proxy o delle VPN. I messaggi di allarme provenienti dal software di sicurezza devono essere controllati immediatamente e devono essere avviate contromisure appropriate.

Ulteriori misure tecniche e organizzative sono riportate nella nostra scheda informativa per le PMI al seguente indirizzo: https://www.ncsc.admin.ch/it-sicherheit-fuer-kmus-it-it

[2] https://www.ncsc.admin.ch/securitytxt-it