Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

Massnahmen zur Cyberresilienz im Kontext von Grossveranstaltungen und internationalen Konferenzen

Grossveranstaltungen und internationale Konferenzen wie beispielsweise das Jahrestreffen des World Economic Forum (WEF) oder die hochrangige Konferenz zum Frieden in der Ukraine vom 15. und 16. Juni 2024 haben einen Einfluss auf die Cyberbedrohungslage. Es besteht eine erhöhte Wahrscheinlichkeit, dass Akteure solche Veranstaltungen als Trittbrett für Cyberangriffe verwenden oder aber auch Teilnehmende und deren Organisationen Ziel von Cyberangriffen werden. Während die Motivation von Akteuren hinter solchen Cyberangriffen und deren Ziele unterschiedlich sind, so sind die Grundschutzmassnamen wie in der normalen Lage. Werden diese umgesetzt, kann eine Vielzahl der potentiellen Cybervorfälle verhindert werden.

Dieses Dokument gibt einen kurzen Überblick über die empfohlenen Grundschutzmassnahmen für Organisationen, im Kontext von Grossveranstaltungen und internationalen Konferenzen. Viele der Empfehlungen sind bereits seit Jahren bekannt und werden mittlerweile auch als «Common Best-Practices» betrachtet. Das Bundesamt für Cybersicherheit (BACS) empfiehlt diese, unabhängig von der aktuellen Cyberbedrohungslage, umzusetzen und verdächtige Aktivitäten dem BACS über das Meldeformular[1] zu melden.

Dieses Dokument behandelt nicht den speziellen Schutzbedarf für direkt involvierte Organisationen. Diese Organisationen müssen neben den hier beschrieben Massnahmen einsatzspezifische Gefährdungen und Anforderungen berücksichtigen.

Prioritäre Massnahmen:

Folgende Massnahmen erweisen sich als besonders effektiv, Cyberrisiken zu minimieren und die Cyberresilienz zu erhöhen:

- **Absicherung von Fernzugängen**
  Alle Fernzugänge wie VPN, RDP, Citrix, usw. sowie sämtliche andere Zugänge auf interne Ressourcen (z. B. Webmail, Sharepoint, usw.) müssen zwingend und konsequent mit einem zweiten Faktor (Zwei-Faktor-Authentisierung – 2FA) oder Passkey abgesichert werden. Dies gilt auch für Zugänge von beispielsweise Lieferanten, Vertragspartnern usw.
- **Patch- und Lifecycle-Management**
  Sämtliche Systeme müssen konsequent und zeitnah mit Sicherheitsaktualisierungen (Updates) versorgt werden. Updates, welche kritische Sicherheitslücken in über das Internet erreichbare Systeme beheben, müssen innerhalb 24 Stunden eingespielt werden. Software oder Systeme, welche vom Hersteller nicht mehr unterstützt werden («End of Life» - EOL), müssen abgeschaltet oder in eine separate, abgeschottete Netzzone verlegt werden.
- **Offline-Backups**
  Erstellen Sie regelmässig Sicherungskopien (Backups) Ihrer Daten. Nutzen Sie dabei das Generationenprinzip (täglich, wöchentlich, monatlich - mindestens zwei Generationen). Stellen Sie jeweils sicher, dass Sie das Medium, auf welchem Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer bzw. Netzwerk physisch trennen und sicher aufbewahren oder verwenden Sie WORM-Speichermedien.

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

Zusätzliche Empfehlungen zum Grundschutz:

Die bereits genannten Massnahmen mindern das Cyberrisiko beträchtlich. Sofern möglich, ist es jedoch empfehlenswert, den Grundschutz mit mindestens folgenden Massnahmen weiter zu festigen:

- **Bekanntmachung der Kontaktmöglichkeit bei Sicherheitsvorfällen**
  Es ist sehr lohnenswert eine Kontaktmöglichkeit bei Sicherheitsvorfällen bekannt zu machen. Dies hilft beispielsweise dem BACS oder den Strafverfolgungsbehörden im Falle einer Alarmierung schnell den Kontakt herzustellen. Es wird empfohlen dazu das security.txt[2] zu nutzen.
- **Aktuell halten des Business Continuity Management**
  Es ist sinnvoll, sich für die Kernprozesse der Geschäftstätigkeit zu überlegen, wie diese von der IT abhängen und wie im Fall eines Ausfalls die Wertschöpfung weiter in Teilen erfolgen kann. Ebenso sollten die Notfall- und Krisenprozesse auf Aktualität geprüft werde. Im Minimum sollte klar sein, wer wen informiert und wer welche Entscheide treffen kann.
- **Einsatz eines DDoS-Schutzes**
  Im Internet exponierte Web-Applikationen, Plattformen oder Systeme, welche für die Geschäftstätigkeit unentbehrlich sind, sollte durch eine Anti-DDoS-Lösung oder durch einen Anti-DDoS-Anbieter geschützt werden. Sprechen Sie hierzu mit Ihrem Internet- oder Hosting-Anbieter über mögliche Lösungen.
- **Einsatz eines EDR/XDR zur Detektion von Anomalien**
  Setzen Sie auf sämtlichen Clients und Server ein EDR (Endpoint Detection and Response) resp. XDR (eXtended Detection and Response) ein, um verdächtige Aktivitäten zu erkennen und zu blockieren.
- **Einschränkung des Zugriffs auf exponierte Systeme**
  Prüfen Sie die Zugriffe auf Systeme, Applikationen und Plattformen, welche im Internet exponiert sind und schränken Sie den Zugriff soweit wie möglich ein. Hierbei hilft beispielsweise der Einsatz von Geo-Blocking oder der Einsatz einer «Allow-Liste» für bestimmte IP-Adressen oder IP- Netze («whitelisting»).
- **Prüfen von sicherheitsrelevanten Logdateien**
  Prüfen Sie sicherheitsrelevante Logdateien wie beispielsweise solche von Antiviren-Software, EDR/XDR, Web-Proxy oder VPN regelmässig und zeitnah auf verdächtige Aktivitäten. Alarmmeldungen von Sicherheits-Software sollten sofort geprüft und entsprechende Gegenmassnahmen eingeleitet werden.

Weitere technische und organisatorische Massnahmen finden Sie in unserem Merkblatt für KMUs unter: https://www.ncsc.admin.ch/it-sicherheit-fuer-kmus

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