Myndigheten för samhällsskydd och beredskap

Foto: MSB/Johnér

2023-03-16 08:00 CET

Viktiga lärdomar från cyberkriget i Ukraina

MSB:s rapport *När kriget kom nära – Årsrapport it-incidenter 2022* visar på viktiga lärdomar om hur Sverige bör förbättra informations- och cybersäkerheten för att stå emot allvarliga cyberincidenter. Att den digitala infrastrukturen blir mer robust är viktigt för det svenska totalförsvaret.

Av de 330 it-incidenter som rapporterades in till MSB under 2022 uppges 41 procent bero på systemfel, 26 procent på misstag och 12 procent på någon form av angrepp. MSB:s bedömning är att många av incidenterna skulle

kunna undvikas med bättre rutiner och kompetensutveckling av personal.

– Det grundläggande systematiska informations- och cybersäkerhetsarbetet inom samhällsviktiga verksamheter måste prioriteras. Om samhällsviktiga tjänster inte fungerar kan det leda till allvarliga konsekvenser för medborgarna. Rapportens djupstudie av cyberkriget i Ukraina visar att mängden cyberangrepp kan öka kraftigt i ett läge av krigsrisk eller höjd beredskap. Sverige måste stå redo, säger Mathias Antonsson, senior handläggare på avdelningen för cybersäkerhet och säkra kommunikationer på MSB.

Tema om cyberkrigföringen mot Ukraina
Ukrainas försvar mot Rysslands cyberkrigföring har aktualiserat vikten av ett motståndskraftigt cyberförsvar även i Sverige. Genom att analysera vilken slags cyberattacker Ukraina utsatts för och hur de försvarat sig, kan MSB dra lärdom om vilken typ av cyberförsvar Sverige behöver ha för att stå emot allvarliga cyberattacker vid höjd beredskap eller krig.

– Trots relativt få inrapporterade cyberangrepp i Sverige får riskerna inte underskattas, särskilt i samband med det allvarliga omvärldsläget. Att kunna stå emot allvarliga cyberangrepp är en viktig del i totalförsvaret eftersom cyberangrepp utgör ett ständigt hot mot alla delar av samhället. Om informations- och cybersäkerhetsarbetet prioriteras och resurssätts har Sverige möjlighet att på kort tid stå mycket bättre rustade än idag, säger Åke Holmgren, chef för avdelningen för cybersäkerhet och säkra kommunikationer på MSB.

Rekommenderade åtgärder
MSB erbjuder vägledningar, metodstöd, kurser och rådgivning till organisationer inom offentlig och privat sektor som vill bli bättre på att skydda viktig information och CERT-SE ger stöd och råd till verksamheter som rapporterar in it-incidenter. Genom att kartlägga leverantörskedjor, undvika beroenden av enskilda tjänster, stärka relevanta samarbeten och planera för alla slags risker kan organisationer begränsa effekterna av it-incidenter.

– Om ledare inom samhällsviktiga verksamheter satsar på det förebyggande arbetet kan systemfel, misstag och enklare angrepp undvikas. För att säkerställa ett starkt cyberförsvar ser MSB att det även behövs mer

omfattande insatser som kräver utredningar, politiska beslut och lagändringar, säger Charlotte Petri Gornitzka, generaldirektör på MSB.

MSB:s samlade rekommendationer för ett stärkt cyberförsvar listas i rapporten som har lämnats in till regeringen den 15 mars. De fem centrala lärdomarna som rekommendationerna baseras på är:

1. Tillsammans är vi starka.
2. Systematiskt informations- och cybersäkerhetsarbete gör stor skillnad.
3. Tillämpa allriskperspektivet.
4. God resiliens avgörande vid hybridkrigföring.
5. Legala hinder hämmar cyberförsvaret.

Här kan du ta del av rapporten När kriget kom nära – Årsrapport it-incidenter 2022

Myndigheten för samhällsskydd och beredskap, MSB, har till uppgift att utveckla och stödja samhällets förmåga att hantera olyckor och kriser. Vi bidrar till att samhället förebygger händelser och att vi är beredda när de inträffar. När en allvarlig olycka eller kris inträffar ger vi stöd. Vi ska också se till att samhället lär sig av det inträffade.

Kontaktpersoner

MSB:s presstjänst
Presskontakt
press@msb.se
010-240 44 44

Anna Wennerström
Presskontakt
Pressansvarig
anna.wennerstrom@msb.se

Elin Bohman
Presskontakt
Pressekreterare
elin.bohman@msb.se