Myndigheten för samhällsskydd och beredskap

2022-12-06 15:36 CET

Rekommendationer med anledning av senaste tidens cybersäkerhetsincidenter

Ett antal cybersäkerhetsincidenter av olika slag påverkar svenska verksamheter för tillfället. Både privata och offentliga aktörer är drabbade. MSB och den nationella funktionen CERT-SE vill uppmana verksamheter till att ha en ökad bevakning av sin it-miljö för att kunna upptäcka avvikelser i ett tidigt skede.

Detta i syfte att kunna motstå och hantera olika typer av cybersäkerhetsincidenter – både angrepp och exempelvis driftstörningar – utan att verksamheten påverkas. I Sverige har både offentlig och privat

verksamhet den senaste tiden drabbats av cybersäkerhetsincidenter, i form av exempelvis utpressningsvirus (ransomware), överbelastningsangrepp (DDoS) men även av generella driftstörningar.

Funktionen CERT-SE vid MSB, som har till uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter, är i kontakt med drabbade aktörer och följer händelserna.

– Vi kan inte kommentera några incidenter specifikt eller uttala oss om eventuella samband mellan den senaste tidens incidenter. Oftast är det andra typer av orsaker än angrepp som ligger bakom parallella it-störningar. Exempelvis att flera verksamheter använder tjänster från samma leverantör eller en produkt som visar sig ha en sårbarhet som utnyttjats brett, Anna Lagerkvist, handläggare cybersäkerhet på CERT-SE.

– Vi ser att det säkerhetspolitiska läget innebär ett ökat intresse och en större medvetenhet kring it-säkerhetsfrågor och att många verksamheter jobbar aktivt med att förbättra sin motståndskraft, säger Anna Lagerkvist.

Det är svårt att helt skydda sig från angrepp, men förebyggande åtgärder som kontinuerligt it-säkerhetsarbete med bra rutiner för säkerhetskopiering och återställning av system samt utbildning av personal, underlättar hanteringen och begränsar skadan. För att undvika driftstörningar och kostnader för nedtid och hantering är det viktigt att löpande att prioritera säkerhetsunderhåll av it-miljön, även om vissa av dessa åtgärder kan innebära kortare avbrott i tjänsterna. Man bör också utforma en kontinuitetsplan för att verksamheten ska kunna bedrivas trots störningar eller bortfall av tillgängliga it-system.

Rekommenderade åtgärder (samtliga är en bedömning som verksamheten själv behöver göra):

- Se till att använda tvåfaktorsautentisering och se över era återställningsrutiner.
- Håll koll på aktiviteten i loggar, på administratörskonton och generellt i it-miljön, för att kunna upptäcka avvikelser i ett tidigt skede.
- Se över vilka tjänster i nätverket som är internetuppkopplade,

inklusive fjärråtkomstlösningar.
- Överväg att stänga av trafiken till de nätverk och applikationer som inte är verksamhetskritiska, samt om trafik från länder som organisationen normalt inte ser trafik från/till bör blockas/geofiltreras.
- Se till att det finns tillräckliga loggar över de tjänster som används och att dessa sparas i minst tre månader, och gärna längre än så.

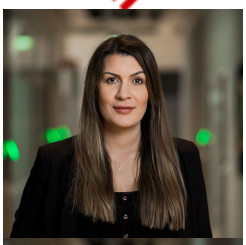
CERT-SE rekommenderar alla verksamheter att se över sin cyberhygien och hur man kan skydda sig som användare. Mer information finns på cert.se: https://www.cert.se/2022/12/cybersakerhetsincidenter-drabbar-svenska-verksamheter-se-over-era-it-miljoer

MSB och funktionen CERT-SE, Sveriges nationella CSIRT (computer security incident response team), har kontinuerlig omvärldsbevakning och samverkan med såväl offentlig som privat sektor. CERT-SE samverkar även med Nationellt cybersäkerhetscenter kring utvecklingen i pågående ärenden. CERT-SE har beredskap dygnet runt om det finns behov av tekniskt stöd eller rådgivning kring pågående incidenter. Vi tar gärna emot utdrag från era loggar och/eller försök till nätfiske om ni upptäcker något misstänkt, mejla då till cert@cert.se. Finns brottsmisstanke bör incidenten även polisanmälas.

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