Enskild motion M1528

SVERIGES RIKSDAG

Motion till riksdagen 2026/27:1361

av Jesper Skalberg Karlsson (M)

Digitala brandövningar

Förslag till riksdagsbeslut

Riksdagen ställer sig bakom det som anförs i motionen om att överväga återkommande övningar i it-säkerhet, exempelvis med simulerade nätfiskemejl vid statliga myndigheter, och tillkännager detta för regeringen.

Motivering

Många minns de brandövningar genomfördes i skolåldern. På ett strukturerat sätt övade man på utrymningsvägar, ansvarsfördelning och handlingsmönster för att veta vad man skulle göra om något inträffade. Den typen av övningar skapar beredskap och kan bidra till att begränsa konsekvenserna av en olycka. Men det svenska samhället behöver också öva mer systematiskt på de risker som följer av den ökande digitaliseringen.

I takt med samhällets digitalisering, där allt fler funktioner och en allt större mängd information hanteras i digitala system, ökar också sårbarheten för cyberangrepp. Nätfiske, dataintrång och överbelastningsattacker utgör återkommande hot mot myndigheter och andra samhällsviktiga verksamheter. Övningar behöver därför vara en återkommande del av myndigheternas säkerhetsarbete.

Den nya cybersäkerhetslagen trädde i kraft den 15 januari 2026 och ställer krav på verksamheter som omfattas av lagen att vidta lämpliga säkerhetsåtgärder för att hantera cybersäkerhetsrisker. Det handlar bland annat om incidenthantering, cyberhygien och utbildning. Återkommande praktiska övningar kan bidra till att omsätta kraven i

fungerande rutiner och stärka organisationernas förmåga att upptäcka och hantera cyberhot.

Karlstads universitet redovisar i sin årsredovisning för 2024 att simulerade nätfiskeattacker genomförts för att förstärka lärandet. Den som klickade fick en kort utbildning i att känna igen och undvika nätfiske. Sådana övningar kan utvecklas till att även pröva om medarbetarna rapporterar misstänkta mejl och om organisationens larmkedja fungerar.

Liknande övningar bör genomföras återkommande hos statliga myndigheter som hanterar känsliga uppgifter eller bedriver samhällsviktig verksamhet. Ett gemensamt metodstöd bör tas fram, så att det sker i enlighet med gällande regelverk och att resultaten kan tolkas och följas upp. En parameter skulle kunna vara hur stor andel av de som klickar på den skadliga länken som också rapporterar händelsen till ansvarig funktion.

Tre principer kan vägleda arbetet med digitala brandövningar. För det första bör medarbetarna känna till att övningar förekommer, även om tidpunkten inte är känd. För det andra bör resultaten användas för lärande och förbättrade rutiner. För det tredje bör uppföljningen omfatta rapportering och organisationens respons, utöver vilka som klickar.

Likt en brandövning ligger värdet i att brister upptäcks och åtgärdas innan en verklig incident inträffar. Nätfiskeövningar kan vara ett sådant initiativ, som ett komplement till tekniska skyddsåtgärder. En vägledande princip behöver också vara just lärandet – skuldbeläggande tester kan skada förtroendet för organisationen och minska viljan att rapportera egna misstag.

Brandövningar i skolåldern fungerar. Samma vana att öva behöver prägla arbetet med IT-säkerhet. Myndigheten för civilt försvars redovisning av Cybersäkerhetskollen i mars 2026 visar att en majoritet av de deltagande offentliga organisationerna inte når nivån för ett systematiskt cybersäkerhetsarbete i respektive delmätning. Det är ett tydligt tecken på att arbetet behöver stärkas. Återkommande praktiska övningar bör därför bli en naturlig del av myndigheternas säkerhetsarbete. Detta bör ges regeringen till känna.

Jesper Skalberg Karlsson (M)