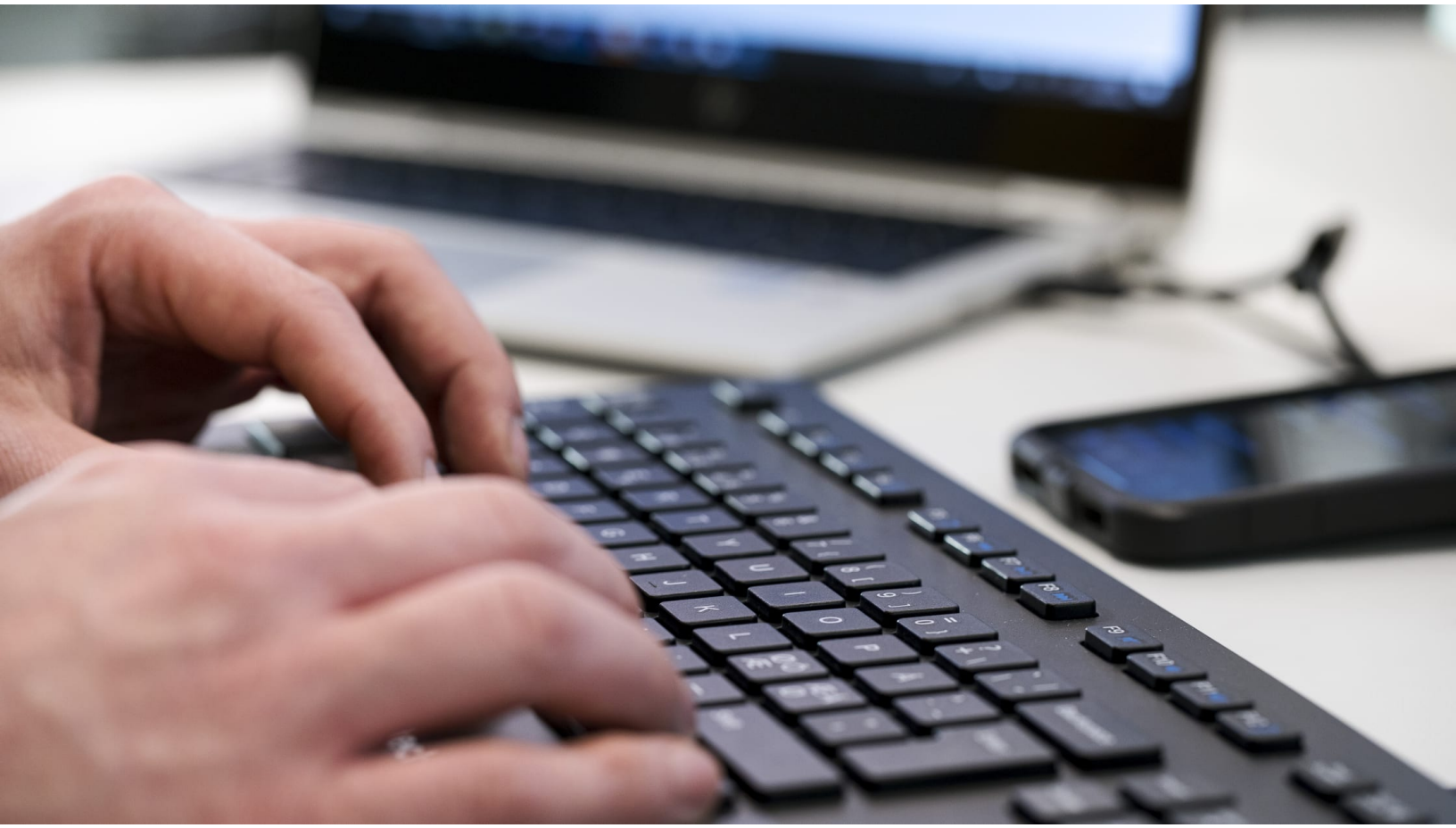
Myndigheten för samhällsskydd och beredskap



2021-11-16 13:26 CET

Ny attackmetod kan drabba användare av Microsoft Exchange

E-posttjänsten Microsoft Exchange har tidigare drabbats av sårbarheter som påverkat användare över hela världen. Nu har en ny attackmetod upptäckts, där användare riskerar att drabbas av ransomware.

Tidigare i år identifierades ett antal olika sårbarheter i Microsoft Exchange, som påverkade användare och verksamheter över hela världen. Nu har en ny attackmetod som utnyttjar dessa sårbarheter upptäckts, som kan innebära risk att bli drabbad av ransomware.

Funktionen CERT-SE vid MSB har fått rapporter om att flera svenska verksamheter är drabbade genom att de fått in ransomware i sina it-system. CERT-SE har varit i kontakt med drabbade och erbjudit tekniskt stöd. CERT-SE bevakar frågan löpande.

Finns det någon rekommendation kring vad man bör tänka på i nuläget?
- Var extremt vaksam på e-postmeddelanden som dyker upp oväntat – det kan röra sig om svar i en existerande mejltråd som dyker upp utan förvarning eller långt efter att konversationen avslutats, e- postmeddelanden som ser konstiga ut på något sätt eller som innehåller någon typ av bilaga, speciellt de som har filändelsen .zip, säger Karl Selin, cybersäkerhetsspecialist i funktionen CERT-SE på MSB.

- Om du är det minsta misstänksam, se till att verifiera filen genom att ta kontakt med avsändaren och/eller informera din it-säkerhetsavdelning, säger Karl Selin.

Organisationer och verksamheter rekommenderas även att tills vidare blockera zip-filer i spamfiltret för att minimera risken för infektion.

Vad är ransomware?
Ett angrepp av ransomware kan innebära att hela eller delar av en verksamhets it-system med dess information blir krypterad och inte är tillgänglig för personalen. Detta kallas ofta för ransomware från engelskans ”ransom” (lösensumma) och ”software” (mjukvara). Genom att kryptera informationen hoppas angriparna på att den utsatta organisationen ska betala en lösensumma för att få tillgång till dekrypteringsnyckeln och få tillbaka den förlorade informationen. I många fall stjäls även information och angriparna hotar med att publicera den känsliga informationen ifall en lösensumma inte betalas.

Vad är CERT-SE?

CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga it-incidenter. Verksamheten bedrivs vid MSB.

---

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
kommunikation@msb.se
010-240 44 44