IT-SÄKERHET OCH MFA

För alla anställda och för politiker

Anders Lagerkvist
IT-chef

2024-02-01

RIKTLINJER FÖR IT-SÄKERHET

Det säkerhetspolitiska läget i Europa har allvarligt försämrats

Efter cyberattacken mot
Norrköpin
”Fortfarar
si
UPPD
I ve
IT-n
helg
– De
stab
tillfö

2023-12-25 00:59 Uppdaterad 2023-12-26 05:07

Misstänkt IT-attack mot Härjedalens

Tieto Evry: Har ingen kontakt med ryska hackarna

It-konsultjätten Tieto Evry, och många av deras kunder, har fallit offer för en storskalig hackerattack.
Sverigechefen Venke Bordal menar att företaget nu befinner sig i en ”krissituation”, men kan inte säga hur lång tid det kommer ta att återställa systemen.

puterSweden

BRANSCH EVENT WHITEPAPERS NYHETSBREV

Dela

t Öland –
t-system

ck, det säger
n har gått upp i
munchefen

samma it-system har utsatts för

ntats data.

Arbetet inom IT-säkerhet skall

- Stärka Härryda kommuns motståndskraft mot IT-säkerhetsincidenter genom att exempelvis begränsa påverkan av skadlig kod eller intrång

- Arbetet skall bidra till att minska risken för informationssäkerhetsincidenter

Riktlinjer IT-säkerhet

IT-säkerhet handlar om att skydda verksamheternas IT-relaterade tillgångar såsom teknisk utrustning, infrastruktur, programvara och verksamhetssystem samt den information som lagras och hanteras i dessa från att nås eller påverkas av obehörig.

Arbetet inom IT-säkerhet och dess skyddsåtgärder ska vara förebyggande så att **informationen är tillgänglig och riktig**.

Arbetet skall bidra till en robust, motståndskraftig och säker IT-miljö

Informationssäkerhet

Information är en av våra viktigaste tillgångar!

”Med informationstillgångar i Härryda kommun avses **all information**, **oavsett** om den **behandlas manuellt** eller **automatiserat** och oberoende av dess **form eller miljö den förekommer i”**

Vad kan påverka informationssäkerheten?

- Var dokument och information lagras
- Åtkomst/Behörighet
- Hur enheter och användare administreras
- Säkerhetsfunktioner (ex MFA)

Från policy för informationssäkerhet:

- Kommunen ska säkerställa informationens tillgänglighet/riktighet/sekretess/spårbarhet
- Hotbilden mot kommunens information, system och teknisk utrustning skall analyseras och hanteras
- Information, system och teknisk utrustning förväntas ha ett skydd i tillräcklig grad
- Det ska finnas tillgång till en gemensam och säker infrastruktur för intern och extern kommunikation

Några exempel på pågående arbete

- ✓ IT-utrustning som ansluts till förvaltningens interna trådlösa administrativa nätverk är administrerad/certifierad/godkänd av IT-funktionen
- ✓ Microsoftlicenser med ökad centraliserad säkerhetsfunktionalitet med exempelvis bättre skydd mot nätfiske, skadliga länkar och bilagor, skadlig kod och misstänkta inloggningsförsök.
- ✓ Utbyggnad av trådlös infrastruktur för bättre tillgänglighet och robusthet
- ✓ Multifaktor (MFA) för administrativ personal och politiker för att verifiera inloggning/identitet och skydda information och system
- ✓ Windows 11 och ändrade lokala behörigheter
- ✓ Backup och brandväggsarkitektur

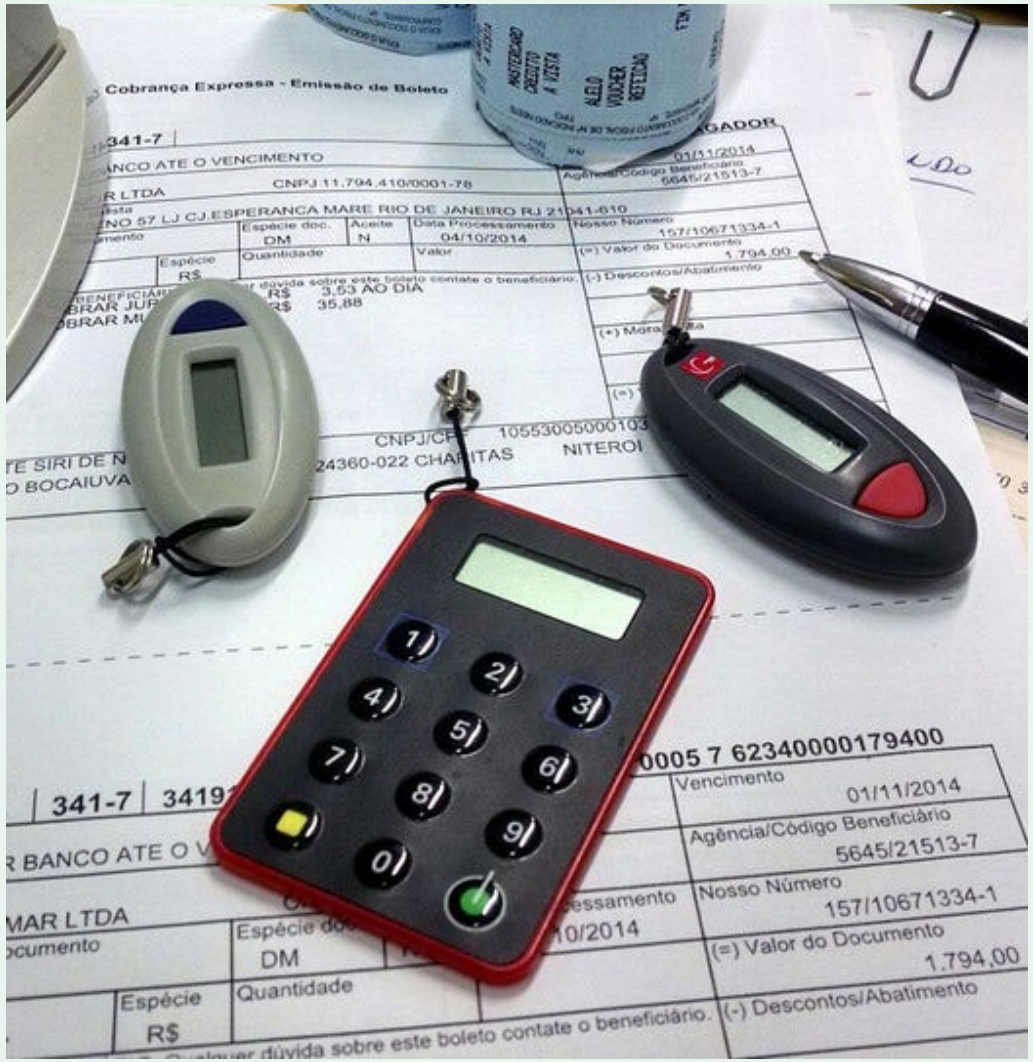
Så vad är multifaktor?

MFA är en teknik och ett extra lager av säkerhet som kompletterar skyddet som ett lösenord ger.

Genom att kunna komplettera en inloggning med en verifieringskod som skickas till en ”applikation” på din läsplatta så säkerställs det i inloggningen att du är den som du utger dig för att vara.

Detta gör det svårare för en obehörig att komma åt ditt användarkonto och din information, även om de skulle ha fått tillgång till ditt lösenord.

Ni kommer att uppmanas att verifiera er identitet när något avvikande inträffar. När något ovanligt sker kopplat till er/en inloggning.



När ni har MFA aktiverat

- Ni loggar in på er läsplatta med en sifferkombination

- Inloggning till Quickchannel och Meeting plus sker precis som vanligt med användarnamn och lösenord
  - Eventuellt kan Härryda kommun längre fram koppla på MFA även vid inloggning till dessa applikationer

- MFA ökar säkerheten med ett extra lager av säkerhet.

  Omständigheterna påverkar i vilka situationer ni kommer att bli uppmanade att verifiera er via MFA. Ni verifierar er via en app som heter Microsoft Authenticator och som kommer att finnas installerad på er läsplatta

- Ni kan fortfarande själva installera applikationer såsom exempelvis andra e-postkonton eller kalendrar på läsplattan. Vi arbetar med att isolera Härryda information till de applikationer dom distribueras ut till er.

Vad blir nästa steg?

Tester har genomförts med kansliet och vi har gått ut med riktad information till några av er inför nästa testfas

- Mer information kommer att skickas till alla er om hur det påverkar er och hur ni använder MFA
  - Mer om MFA och förberedelser (bland annat ett formulär)
  - Hur ni aktiverar MFA
    - Aktivering sker med hjälp av ert mobilnummer och er mobiltelefon (kod). Detta för att identifiera er när MFA aktiveras (även vid ett eventuellt kommande byte till en ny läsplatta).
  - Hur ominstallationen av er läsplatta går till

- Informationen på er läsplatta kommer att raderas. Inför ominstallationen så behöver ni säkerställa exempelvis säkerhetskopiering av bilder och att ni känner till lösenord till egna appar, apple-id etc

- Eventuella egna appar behöver installeras om (av er). Appar som Härryda IT distribuerar ut, exempelvis M365 kommer att installeras automatiskt (även Quickchannel och Meeting plus)

- Ominstallationen planeras till den 20 – 22 februari. Den 20e och 21e kan ni själva starta ominstallationen (rekommenderas). IT-funktionen kommer att initiera ominstallationen av era läsplattor på distans den 22e. Ni behöver inte vara i kommunhuset för att installera om läsplattan, det kan ske på distans förutsatt att läsplattan är uppkopplad på ett trådlöst nätverk och internet

- Medarbetare från IT-funktionen kommer att finnas tillgängliga under tre dagar för att hjälpa er i kommunhuset (20 – 22e)

Tillägg

Några exempel på när MFA (Microsoft Authenticator) kommer att begära att ni identifierar er är när:

Något ovanligt inträffar i samband med en inloggning. Exempelvis vid:

- inloggning från utlandet
- flera samtidiga inloggningsförsök (kapat konto)
- byte av lösenord på ert användarkonto på annan enhet än er tilldelade läsplatta

Så sammanfattningsvis. I er vardag så kommer ni inte att få uppsärskilt många uppmaningar om att identifiera er via MFA. Men det extra lagret av säkerhet finns där hela tiden för att fånga upp misstänkta inloggningsförsök

Frågor?