Ansatte og IT-sikkerhet

IT-sikkerhet handlet lenge om å ha oppdatert virusprogramvare og brannmurer. I dag er oppmerksomme og bevisste medarbeidere like viktig i arbeidet med å beskytte bedriften mot digitale angrep og informasjon på avveie.

Technical manager
Arne Klæboe
Head of Technical Security i Intility

Man har sett en jevn økning i angrep mot IT-systemene til norsk næringsliv og forvaltning de siste årene, og det er lite som tyder på at denne tendensen svekkes med det første. De store og spektakulære angrepene får offentligheten ofte høre om, men majoriteten av angrepene blir aldri rapportert eller kommunisert. I tillegg finnes det et stort antall tilfeller som heller ikke blir oppdaget. Til sammen er dette en trussel som norsk næringsliv og forvaltning må ta alvorlig, og beskyttelsen starter ofte med hver enkelt ansatt.

Ansatte er sikkerhetsansvarlig

En stor sikkerhetsutfordring er at mange ansatte gjerne tenker at sikkerhet kun er ansvaret og oppgaven til de som har sikkerhet nevnt i egen stillingsbetegnelse. Slik er det ikke. En bedrifts sikkerhetskultur er ikke bedre enn den enkelte medarbeiders ivaretakelse av egen datasikkerhet. Sikkerhetskulturen kan altså bare forbedres gjennom å forstå at man selv har et ansvar.

Bevissthet om eget ansvar gir god sikkerhetskultur

En bevissthet rundt denne problemstillingen og egen brukeratferd, er antageligvis der det er mest å hente innen sikring, spesielt av mobile enheter. Moderne mobilplattformer har som oftest solide mekanismer for å beskytte data på enheten. Det hjelper imidlertid lite om brukerne ikke tar enkle forholdsregler.

Beredskapsøvelser – like vanlig som brannøvelser?

At digitale trusler og angrep mot norske bedrifter vil fortsette å øke i tiden fremover, er både kjent og forventet. Behovet for å øke den interne beredskapen og dermed styrke sikkerhetskulturen i organisasjonen er hva det i bunn og grunn handler om. En mulig aktivitet er å gjennomføre beredskapsøvelser, der bedriften bruker et sikkerhetsselskap til å gjennomføre tester basert på phishing-teknikker for å få tilgang til en brukers pc, og herfra se hvilken

Sikring av mobile enheter

- Passord/låsekode: Sikre at ikke andre får tilgang til innholdet
- Bruk totrinns bekreftelse/multi-faktor autentisering på alle tjenester der det er mulig. BankID krever for eksempel to ting for å logge inn; noe du vet (passord) og noe du har (passordkalkulator eller mobiltelefon)
- Fysisk kontroll: Unngå at enheten kommer i feil hender.
- Sikkerhetsoppdateringer: Unngå sikkerhetshull.
- Sikkerhetskopiering.
- Sikrede trådløse soner: kjennetegnes ved at de krever passord.
- Kryptering (hvis mulig): Særlig når det gjelder sensitive data.
- Automatisk sletting av data: Ved frastjålet enhet.
- Sporingsprogram: Vil kunne se hvor enheten er på et kart, låse den og slette innholdet over nettet.
- Vurder hvilke applikasjoner som lastes ned/benyttes.

E-post svindel: Hva skal ansatte være oppmerksomme på?

- Forventer du e-posten?
- Sjekk avsenderadresse.
- Mottar du linker? Hold musepekeren over linken for å se hvor URL'en peker hen.
- Dårlig språk og grammatikk.
- Spørsmål/innhenting av personlig informasjon.
- Vedlegg og bilder i e-post.
- Varsel om kjøring av fil.
- Bruk av tillit, tidspress og trusler.

informasjon man klarer å få tilgang til videre inn i organisasjonen. Slike tester, såkalte penetrasjonstester, er noe flere begynner å se på som like naturlige som brannøvelser. Ansatte bør ha kunnskap om sikringstiltak mot digitale trusler, og være kjent med arbeidsplassens interne retningslinjer for IT-sikkerhet. Når kunnskapen hos de ansatte øker, øker også sikkerheten i bedriften.

Mobilitet

De samme dataene som tidligere kun var på PC'en, har dagens løsninger tilgjengeliggjort på øvrige enheter som mobil og nettbrett. Dette gir brukerne ekstra ansvar i forhold til sikkerhet fordi utstrakt bruk av enheter gjør angrepsoverflaten desto større og gir flere kilder for tap av informasjon. Mange ansatte kan i dag også velge hvilken enhet de ønsker å bruke i jobbsammenheng, slik at de eventuelt også kan velge å bruke private enheter i jobbsammenheng. Om dataene kan ansees som sensitive, må spesielle forholdsregler tas.

E-post svindel

De klassiske hackerangrepene, angrep rettet mot systemer og tjenester, såkalte systemangrep, handler om å finne svakheter i maskin- og programvare; sikkerhetshull som kriminelle kan utnytte for å komme seg på innsiden av bedriftens IT-løsning. Dette er fortsatt en del av trusselbildet, men samtidig har det skjedd en dramatisk økning i det man kaller «brukerangrep» eller sosial manipulasjon. Svindel ved utnyttelse eller bruk av e-post har hatt en kraftig økning, og svindlerne blir stadig mer profesjonelle og utspekulerte i sine metoder og fremgangsmåter. Alle som har en e-post konto, enten privatpersoner eller bedrifter, kan være potensielle målgrupper for denne typen svindel. Tendensen er at dagens sikkerhetstrusler blir mer tilpasset målgruppen, utforming og språk blir proffere og det blir dermed vanskeligere å avsløre om avsenderen er den vedkommende utgir seg for å være eller ikke.

Løsepengevirus (Ransomware)

Løsepengevirus er en type skadevare som låser eller krypterer hele eller deler av maskiner eller filservere. Kjente eksempler er blant annet Cryptolocker, TorrentLocker og Cryptowall. Skadevaren blir ofte spredd via utdatert programvare eller som vedlegg i e-poster. Dette forårsaker nedlåsing og kryptering av filer både lokalt på disken, men også på felles områder den infiserte maskinen har tilgang til. Målet med angrepet er å få brukeren til å betale løsepenger, ofte innen en gitt tidsfrist, for å få tilbake tilgang til filene sine. Det blir oppdaget nye krypteringsvirus på markedet stadig vekk, og så lenge ofrene fortsetter å betale, er det rimelig å tro at disse angrepene vil fortsette.

Nettfiske (phishing)

Nettfiske er tilfeller der svindleren utgir seg for å være en reell, troverdig virksomhet, for eksempel Posten, en bank eller et kredittkortselskap. Denne formen for e-postsvindel regnes ofte som den mest effektive metoden, da den treffer bredt ved at den sendes til en rekke mottakere. E-posten opplyser typisk om at det har oppstått et problem og at dette løses ved at mottaker følger noen instrukser. Mottakeren kan lures til å åpne et vedlegg eller klikke seg inn på en falsk nettside for å «logge» seg inn eller oppgi annen sensitiv informasjon som passord, konto- eller kredittkortnummer. Svindleren benytter disse opplysningene i et forsøk på å gjennomføre en eller annen form for svindel.

CEO/direktør-svindel

CEO-svindel er en form for e-postsvindel som har hatt en særskilt økning det siste året. Til forskjell fra løsepengevirus og nettfiske, retter CEO-svindel seg mot en spesifikk person, med en spesifikk rolle. CEO-svindel utføres ved at personer utgir seg for å være en leder (gjerne administrerende direktør) i et selskap, og tar kontakt med en underordnet i selskapet via e-post. Svindleren har til hensikt å få mottakeren, som typisk er en med myndighet til å utføre transaksjoner (f.eks. CFO), til å betale en faktura eller overføre en sum med penger til et gitt kontonummer, ofte til utlandet. Avsenderens e-postadresse ser tilsynelatende ekte ut, men hvis mottaker velger å svare, blir svaret sendt til svindlerens e-postadresse og ikke til direktørens e-postadresse som står i avsenderfeltet. CEO-svindlere blir stadig grundigere i sin kartlegging og klarer å identifisere navn på nøkkelpersoner i bedriften. I tillegg oppretter svindlerne domener med bedriftens navn for å kunne opprette e-postadresser som ligner på de bedriften allerede har. E-postene er ofte dyktig formulert på norsk, og signert slik «direktøren» vanligvis gjør. Disse elementene resulterer i at CEO-svindel fremstår som mer troverdig, og har vist seg å være effektivt da flere selskaper, også i Norge, har latt seg lure av disse målrettede angrepene.

Dette kan ansatte og bedriften gjøre

Det finnes flere ting som både bedriften og ikke minst hver enkelt bruker kan gjøre for å begrense mulighetene for og de eventuelle skadene av slike angrep:

- Forsikre seg om at brukernes klienter (PC, mobiler, nettbrett m.m.) oppdateres jevnlig, både hva gjelder operativsystemet og de enkelte programmene: Det er den enkleste måten å beskytte seg mot virus.
- Sørge for at bruker og bedrift har gode sikkerhetsprogramvarer på både klienter og IT-systemene.
- For en eventuell IT-avdeling eller tjenesteleverandør gjelder det å ha sikre soner, brannmurer, antivirusløsninger og automatiske oppdateringer av programvare
- To-faktor autentisering av alle IT-tjenestene er også en god måte å sikre at uvedkommende ikke får tilgang til bedriftens kritiske systemer
  - Dette gjelder for øvrig også sosiale tjenester som Facebook, Google+ m.m.
- Proaktiv overvåking/deteksjon: Overvåkingssystemer for oppdagelse av uønskede hendelser.
- Og sist, men ikke minst – ikke glem å bruke sunn fornuft!
  - Ting som virker for godt til å være sant er ofte det
  - Unngå å åpne ukjente vedlegg eller klikke på lenker
  - Still alltid spørsmålstegn ved troverdigheten til ukjente avsendere og vedlegg
  - Og skulle man bli utsatt for et angrep; si ifra med en gang til IT- eller sikkerhetsansvarlig i bedriften. Tid er svært viktig i slike tilfeller.