Ctrl Alt Konsult AB

Uppföljning föreläsning på frågorna som ställdes efter mitt föredrag 10/2 samt lite tips på vägen, detta brev är utan länkar utan bara tips och förslag.
Lite förklaringar på de olika hotbegreppen jag pratade om i en lite mer ingående information.

Tvåfaktorsautentisering innebär att din inloggning sker i två steg. Efter att ha fyllt i ditt användarnamn och lösenord måste du bevisa din identitet på ett annat sätt. Det kan till exempel ske med en kod från ett textmeddelande, en personlig fråga, ditt fingeravtryck eller en app. Med hjälp av tvåfaktorsautentisering hindrar du obehöriga hackare från att få tillgång till ditt konto. Tvåfaktorsautentisering kan även kallas tvåfaktorsverifiering eller förkortas 2FA från engelskans two-factor authentication eller MFA från multi-factor authentication.

Hur fungerar tvåfaktorsautentisering?

Vid inloggning till ett konto bekräftas användarens identitet traditionellt med användarnamn och lösenord. Dessa kan vara lätta att klura ut och därför ger inte användarnamnet och lösenordet ett tillräckligt skydd mot onlinebrottslingar. Användarnamnet är ofta personens e-post och är därför inte svårt att gissa. Många användare brukar även ha samma lösenord till flera konton. Du ska inte återanvända ett lösenord eftersom en brottsling då lätt kan komma åt flera av dina konton samtidigt.
För att undvika att svaga inloggningskoder knäcks har flera tjänster tagit i bruk tvåstegsautentisering. I många fall är tvåstegsautentisering inte en standardinställning, utan användaren aktiverar tjänsten manuellt från kontots inställningar. Därefter frågas önskad typ av tvåstegsverifiering vid varje ny inloggning eller ny enhet. För maximalt skydd rekommenderar vi att du aktiverar tvåfaktorsautentisering på så många användarkonton som möjligt. Metoderna för tvåfaktorsautentisering kan i stora drag delas in i tre kategorier:

- **Något som du vet**, till exempel en PIN-kod eller en personlig fråga.
- **Något som du har**, till exempel en telefon eller ett kreditkort.

- **Något som du är**, till exempel biometriska mönster eller ett fingeravtryck.

Varför ska jag ha tvåstegsautentisering?

En ständig ökning av onlinebrottslighet är ett faktum och därför måste du se till att ingen annan än just du kan logga in på dina användarkonton. Termen tvåfaktorsautentisering kan låta komplicerad och för att förtydliga dess innebörd listar vi fyra nyttor av tvåstegs-autentiseringen:

- **Förhindra kontoövertaganden**. Om en onlinebrottsling lyckas bryta sig in på ditt konto kan hen stjäla dina personliga uppgifter, till exempel bankkoder, och använda dem för att köpa eller sälja något online.
- **Förhindra identitetsstöld**. I samband med kontoövertagning kan du även bli utsatt för identitetsstöld. Följderna kan bli allvarliga och dyra om du inte får hjälp i tid.
- **Förhindra bedrägeri i ditt namn**. Om en brottsling kommer åt ditt konto på till exempel sociala medier kan hen utnyttja det för att sprida falska meddelanden i ditt namn. Som exempel kan bedragaren ta över ditt Instagram konto och försöka sälja bitcoins till dina följare.
- **Ta hand om dina konton**. Genom att aktivera tvåstegsautentisering tvingas du att fundera noggrannare på din onlinesäkerhet. Många använder samma lösenord till flera konton och för att eliminera denna säkerhetsrisk är tvåstegsautentisering ett effektivt sätt att öka medvetenhet om sekretess på nätet.

Olika typer av tvåfaktorsautentisering

Baserat på de tre ovannämnda kategorierna listar vi olika typer av tvåfaktorsautentisering.

- **Personlig fråga**. I samband med inloggningen ber enheten dig svara på någon personlig fråga som bara du kan veta svaret på.
- **Engångslösenord eller bekräftelsenummer**. Du får en PIN-kod via SMS med en ny kod som bekräftar din identitet varje gång du loggar in.
- **Face-ID**. Enheten måste läsa av ditt ansikte för att vara säker på att det är du som loggar in.
- **Fingeravtryck**. Eftersom allas fingeravtryck är olika skannar du ditt finger för att komma in. Moderna smartphones stöder denna inloggningsmetod och kan avläsa ditt fingeravtryck via mobilens skärm.

- **Röstigenkänning**. Inloggningen kräver att enheten känner igen din röst innan du får tillgång till kontot. Var uppmärksam eftersom röstigenkänning kan förfalskas med förinspelade snuttar av den riktiga användarens röst.
- **QR-kod**. För att logga in måste du avläsa en QR-kod med en app eller med din enhet.
- **Autentiseringsapp**. Till exempel banker brukar använda en skild autentiseringsapp för att kunna logga in.
- **Skyddsnyckel eller token**. Fysiska enheter, till exempel USB-, NFE- eller Bluetooth-enheter, som bekräftar din identitet.

Hur kan hackare kringgå tvåfaktorsautentisering?

Även om 2FA förstärker skyddet av onlinekonton och gör det svårare för brottslingar att hacka sig in på dem finns det fortfarande sätt att kringgå tvåfaktorsautentisering.

Social engineering

Social engineering, även kallat social manipulation, innebär att en cyberkriminell person försöker lura eller övertyga en användare att uppge sekretessbelagd information för att kunna ta över kontot. Onlinebrottslingarna utnyttjar alltså en av de svagaste länkarna i cybersäkerheten: offren själva. En vanlig typ av social engineering är nätfiske där bland annat e-post används för att lura människor eller infektera deras enheter med malware. För att kringgå tvåfaktorsautentisering kan en onlinebrottsling påstå sig vara en trovärdig och auktoritär person eller organisation. På så sätt försöker brottslingen få offret att uppge nyckeln för tvåfaktorsautentisering. Om bedragaren redan har fått tag på offrets användarnamn och lösenord kan hen bryta sig in på kontot med hjälp av 2FA-nyckeln.

Brute force

Inom cybersäkerhet innebär så kallade brute force -attacker upprepade försök att logga in på ett konto. Försöken görs ofta med hjälp av någon typ av programvara som försöker gissa ett kontolösenord. Med svagt lösenord och ingen gräns för hur många gånger en användare kan ange felaktigt lösenord kommer en onlinebrottsling förr eller senare in på kontot. Ju längre och mer komplicerat lösenord, desto längre tid tar det att knäcka det med brute force.

Samma princip gäller för 2FA-koder. Om koden är kort, bara fyra till sex siffror, kan den knäckas med brute force. För att förhindra detta brukar koden vara aktiv endast under en kort tid eller så begränsas autentiseringen av endast ett fåtal misslyckade försök.

Token

Många typer av tvåfaktorsautentisering ger den nyckel, eller token, som används för autentisering i samband med inloggningen. I vissa fall finns det ändå en lista över tokens som utsetts i förväg. Bedragaren måste då veta vilken token som ska användas för att kunna kringgå tvåfaktorsautentisering. Hen måste även få tag på offrets användarnamn och lösenord.

Malware

Cyberkriminella kan använda sig av malware för att kringgå tvåfaktorsautentisering och få tillgång till offrets konton. Till exempel en del avancerade Android-banktrojaner verkar vara legitima bankappar, men i verkligheten lurar de offret att själv autentisera åtkomst år brottslingen. Liknande skada kan även orsakas av malware i till exempel tjänster för kryptovalutor.

Ändra offrets säkerhetsinställningar

Ett engångslösenord eller ett bekräftelsenummer skickas ofta till användarens mobiltelefon i samband med tvåfaktorsautentisering. Om en onlinebrottsling lyckas ändra på offrets säkerhetsinställningar kan hen kringgå detta steg i autentiseringen. En hackare kan till exempel ändra på telefonnumret som bekräftelsekoden skickas till och få den skickad till sin egen telefon istället för den riktiga kontoinnehavarens telefon.

Att ställa in 2-faktors autentisering på enheterna

Apple

Aktivera tvåfaktorsautentisering för ditt Apple-ID

Om du inte använder tvåfaktorsautentisering för ditt Apple-ID kan du aktivera det direkt på enheten eller på webben:

- På din iPhone, iPad eller iPod touch: Gå till Inställningar > ditt namn > Lösenord och säkerhet. Tryck på Aktivera tvåfaktorsautentisering. Tryck sedan på Fortsätt och följ anvisningarna på skärmen.
- På din Mac: Välj Apple-menyn > Systeminställningar och klicka sedan på ditt namn (eller Apple-ID). Klicka på Lösenord och säkerhet. Bredvid tvåfaktorsautentisering klickar du på Slå på och följer anvisningarna på skärmen.
- På webben: Gå till appleid.apple.com och logga in med ditt Apple-ID. Svara på dina säkerhetsfrågor och tryck sedan på Fortsätt. Tryck på Fortsätt när du ser en uppmaning om att uppgradera kontots säkerhet. Tryck sedan på Uppgradera kontots säkerhet och följ anvisningarna på skärmen.

Om du redan använder tvåfaktorsautentisering med ditt Apple-ID kan du inte stänga av det. Om du uppdaterade till tvåfaktorsautentisering av misstag kan du stänga av det inom två veckor efter registreringen. Om du gör det är ditt konto mindre säkert och du kan inte använda funktioner som kräver en högre säkerhetsnivå.

Första gången du loggar in med ditt Apple-ID på en ny enhet

När du loggar in med användarnamnet för ditt Apple-ID och lösenord för första gången på en ny enhet eller webben får du ett meddelande på dina betrodda enheter om att någon försöker logga in med ditt Apple-ID. Meddelandet kan innehålla en karta över den ungefärliga platsen för inloggningsförsöket. Den platsen baseras på den nya enhetens IP-adress och kan återspegla nätverket som den är ansluten till, snarare än den exakta fysiska platsen. Om du vet att du är den person som försöker logga in men inte känner igen platsen kan du fortfarande trycka på Tillåt och visa verifieringskoden. Om du inte är den som försöker logga in trycker du på Tillåt inte för att blockera inloggningsförsöket.

Google

Aktivera tvåstegsverifiering

1. Öppna Google-kontot.
2. Välj Säkerhet i navigeringspanelen.
3. Välj Tvåstegsverifiering under Logga in på Google. Kom igång.
4. Följ anvisningarna på skärmen.

Facebook

Aktivera eller hantera tvåfaktorsautentisering

1. Gå till inställningarna för säkerhet och inloggning.
2. Bläddra ned till **Använd tvåfaktorsautentisering** och klicka på **Redigera**.
3. Välj den säkerhetsmetod som du vill lägga till och följ anvisningarna på skärmen.

När du konfigurerar tvåfaktorsautentisering på Facebook blir du uppmanad att välja en av tre säkerhetsmetoder:

- genom att trycka på säkerhetsnyckeln på en kompatibel enhet
- med inloggningskoder från en autentiseringsapp från tredje part
- med sms-koder från din mobiltelefon.

När du har aktiverat tvåfaktorsautentisering kan du få tio återställningskoder för inloggning som du använder när du inte har tillgång till din telefon. Ta reda på hur du konfigurerar återställningskoder.

Andra användbara resurser

- Om du inte har sparat webbläsaren eller den mobila enheten som du använder uppmanas du att göra det när du aktiverar tvåfaktorsautentisering. Då behöver du inte ange en säkerhetskod när du loggar in igen. Klicka inte på **Spara den här webbläsaren** om du använder en offentlig dator som andra kan få tillgång till (exempelvis en dator på ett bibliotek).

- Vi måste kunna komma ihåg din dator- och webbläsarinformation så att den känns igen nästa gång du loggar in. Vissa webbläsarfunktioner blockerar denna igenkänning. Om du har aktiverat privat surfning eller ställt in webbläsaren så att historiken rensas varje gång webbläsaren stängs ner kan du behöva ange en kod varje gång du loggar in. Ta reda på mer.
- För att konfigurera tvåfaktorsautentisering för textmeddelanden (SMS) kan du antingen använda ett mobilnummer som redan har lagts till på ditt konto eller lägga till ett nytt nummer. Ta reda på mer om hur Facebook använder ett mobilnummer som har lagts till för tvåfaktorsautentisering.
- Ta reda på vad du kan göra om du har inaktiverat tvåfaktorsautentisering men nu har problem med att logga in.

Instagram

Hur aktiverar eller inaktiverar jag tvåfaktorsautentisering på Instagram för flera enheter?

Kopiera länk

Om du konfigurerar tvåfaktorsautentisering för ett Instagram-konto med en autentiseringsapp från tredje part kan du ansluta flera enheter till tvåfaktorsautentisering på det kontot.

När du lägger till flera enheter till tvåfaktorsautentisering på ett enskilt Instagram-konto får du en sexsiffrig inloggningskod från autentiseringsappen på den enheten.

Tänk på att en enhet måste konfigurera tvåfaktorsautentisering via en autentiseringsapp innan andra enheter kan läggas till. Eventuella ytterligare enheter måste också ladda ned en autentiseringsapp innan de ansluts till tvåfaktorsautentisering.

Så här konfigurerar du tvåfaktorsautentisering på fler enheter:

1. Ladda ned en autentiseringsapp från tredje part från den enhet som du vill lägga till (till exempel: Duo Mobile, Apple Passwords eller Google Authenticator) och öppna sedan Instagram-appen från den enheten.

2. Tryck på  eller din profilbild längst ned till höger för att gå till din profil.

3. Tryck på  längst upp till höger och tryck sedan på  **Inställningar**.
4. Tryck på **Sekretess** och tryck sedan på **Tvåfaktorsautentisering**.
5. Tryck på  bredvid **Autentiseringsapp** och tryck sedan på **Lägg till**.
6. Namnge enheten som du lägger till och tryck sedan på **Nästa**.
7. Tryck på **Kopiera nyckel** och klistra sedan in den i autentiseringsappen.
8. När Instagram-kontot har kopplats till autentiseringsappen kopierar du den sexsiffriga koden som autentiseringsappen genererar.
9. Gå tillbaka till Instagram-appen, tryck på **Nästa** och klistra in den sexsiffriga koden för att slutföra processen på den enheten.

Tänk på att du kan lägga till upp till fem anslutna enheter till tvåfaktorsautentisering för ett enskilt Instagram-konto och att du när som helst kan ta bort en ansluten enhet.
Så här tar du bort en ansluten enhet från tvåfaktorsautentisering:

1. Tryck på  eller din profilbild längst ned till höger för att gå till din profil.

2. Tryck på  längst upp till höger och tryck sedan på  **Inställningar**.
3. Tryck på **Sekretess** och tryck sedan på **Tvåfaktorsautentisering**.
4. Tryck på  till höger om enheten som du vill ta bort.
5. Tryck på **Ta bort**. Obs! Om du tar bort den anslutna enheten från tvåfaktorsautentisering loggas den inte ut från ditt konto.

Obs! Din Instagram-nyckel kan också användas om du använder flera autentiseringsappar på samma enhet. För att göra detta följer du stegen här ovan på samma enhet.

Lite förklaringar på olika hot

Varför är malware ett hot mot dig?

Begreppet malware härstammar från de engelska orden malicious software och används som benämning för skadlig programvara. Alla typer av malware har ett gemensamt karaktärsdrag: de är skapade för att skada det infekterade systemet. Brottslingar på nätet sprider malware för att utföra cyberattacker. Majoriteten av dagens malware sprids online men skadliga programvaror har använts redan långt innan flera enheter var uppkopplade online.

Målet med malware är att utnyttja en infekterad enhet för att få tag på sekretessbelagd information eller åstadkomma annan skada. Bank-id, kontonummer, personuppgifter eller användarkoder kan hamna i fel händer utan att den drabbade är medveten om det. Malware drabbar inte bara datorer, utan också mobila enheter, såsom smartphones, är lika frestande måltavlor för brottslingar.

De största hoten som orsakas av malware är:

- Stöld av kreditkortsinformation eller pengar från ditt bankkonto
- Stöld av personlig information för identitetsstöld eller utpressning
- Stöld av lösenord och inloggningsuppgifter för kontoövertagning
- Låsa eller kryptera din enhet eller dina filer och kräva lösensumma
- Förstöra filer och raderar data
- Stöld av känsliga och personliga bilder
- Samla in information om din arbetsplats och dess system
- Tvinga din enhet att sprida malware eller spam till andra enheter
- Användning av din enhet för att tjäna på kryptovalutor
- Spionering av de webbplatser du besöker eller vad du skriver på tangentbordet
- Användning av din enhet för att utföra DDoS-attacker

Olika typer av malware

Fastän teknologin för att bekämpa skadlig programvara blir bättre, betyder det inte att hoten blir enklare att undvika. Brottslingar, hackare och statligt finansierade organ kommer ständigt på nya former av malware. För att kunna skydda dig bör du vara medveten om olika typer av malware samt deras karaktärsdrag.

Virus

Datorvirus är bland de vanligaste och mest kända formerna av malware. Viruset smittar skadlig kod från en dator till ett annat datorprogram, vanligen genom att utnyttja en befintlig säkerhetsbrist i programmet. Koden börjar fungera när det infekterade programmet används. Detta kan leda till att den infekterade enhetens minne korrumperas och utplånas eller att den inte kan startas.

Trojan

Det trojanska viruset ser ut som ett vanligt datorprogram, men egentligen lurar programmet åt sig dina privata uppgifter, spionerar på dig eller kraschar din enhet. Trojanen kan gömma sig i till exempel ett mejl och kan infektera din enhet med flera elakartade program samtidigt.

Ransomware

Ransomware kallas också gisslanprogram eller untpressningstrojan. Brottslingar använder ransomware för att kryptera filer eller användarkonton så att ägaren inte längre har tillgång till dem. För att låsa upp dem måste du betala en lönesumma i utbyte. Bedragare föredrar kryptovalutor, till exempel bitcoin, som betalning eftersom de är svårare att spåra. Det finns ingen garanti på att du får tillbaka dina filer genom att betala lösensumman, så kontakta dina lokala myndigheter istället för att betala.

Spionprogram

Spionprogram används för att följa upp kommunikation, surfhistorik och annan trafik på en enhet. Spionprogrammen utför ofta sitt arbetet så tyst i bakgrunden att användaren inte märker något. Så kallade keyloggers kan spåra vad du skriver på datorns tangentbord för att stjäla lösenord och inloggningsuppgifter. Spionprogram kan också användas för inspelning av din skärm med målet att utföra identitetsstöld eller kontoövertagning.

Datormask

Datormasken är en typ av malware som enkelt replikerar sig från en enhet till en annan. Masken utnyttjar säkerhetsbrister i operativsystemet och sprids till exempel via datornät-verk. En datormask kräver inga mänskliga handlingar, så som klickande, för att orsaka skada.

Hur skyddar jag mig från skadlig programvara?

Som du precis lärt dig finns det flera typer av malware och därmed även olika sätt att skydda sig med. Vissa skadliga program kan hanteras på specifika sätt, men det finns vissa saker du

kan göra för att förbättra din övergripande informationssäkerhet mot dem alla. Nedan följer en lista på våra bästa tips för att hålla malware borta från dina enheter.

- **Använd ett antivirusprogram**. Antivirusprogrammet skyddar både dina datorer och mobila enheter.
- **Uppdatera ditt operativsystem och dina appar regelbundet**. Uppdateringarna åtgärdar fel och brister som brottslingar tidigare kan ha använt sig av för att ta över din enhet.
- **Överväg vilka program du laddar ner**. Mobila enheter kan generellt anses vara säkra eftersom programmen installeras från enhetens officiella appbutik. Var ändå på din vakt när du laddar ner något och välj programmen varsamt.
- **Klicka inte på okända länkar** i mejl, SMS eller på sociala medier eftersom du kan vara ett offer för nätfiske. Fundera också på om länken ser ut att beskriva den ifråga-varande hemsidan och dess innehåll.
- **Sätt inte in okända hårdvaror i din dator**. Malware kan gömma sig även i USB-minnen, CD-skivor eller andra externa enheter. Se till att du inte ansluter okända enheter till din dator eller låter någon du inte litar på ansluta sin telefon till din enhet.
- **Ha koll på användarrättigheterna som en app eller en programvara kräver**. Många mobilappar kräver tillgång till telefonens kamera, adressbok, platsinformation och sparade filer. Olika typer av malware kan enkelt gömma sig bland villkoren, så läs dem noga.
- **Var på din vakt när du surfar offentligt**. Undvik att utföra e-handel eller logga in i din bank om du sitter på ett café och använder en allmän Wi-Fi. Om du måste logga in någonstans, använd en VPN istället.
- **Använd en brandvägg**. En brandvägg fungerar som ett filter mellan din enhet och internet. Den stoppar misstänkt och potentiellt skadlig nätverkstrafik. Även om en brandvägg kan stoppa hackare och virus behöver den ett antivirusprogram som stöd.

7 enkla tips för att känna igen malware

Malware kan vara svårt att känna igen eftersom den inte kräver mänsklig aktivitet för att åstadkomma skada. Vi har samlat ihop några tips som hjälper dig att känna igen malware i olika kontext.

1. Oväntade popup-fönster i din webbläsare
2. Din enhet är långsammare än vanligt
3. Svårigheter med att starta eller stänga av enheten
4. Din enhets dataanvändning ökar märkbart utan orsak
5. Program, appar eller hela din enhet kraschar oväntat
6. Din enhets batteri laddas ur snabbare än vanligt
7. Din enhet överhettas lätt

Alla enheter blir långsammare när de används och kan nödvändigtvis inte hålla batteriet laddat lika länge som tidigare. Se ändå till att ålderstecken inte orsakas av skadlig kod. Om du märker något av dessa tecken ska du utföra en viruskontroll på din enhet. Detta är en enkel process som körs med hjälp av avancerad säkerhetsprogramvara.

Malware i Sverige

Annonsbluffar blir allt vanligare och under det senaste decenniet har borttagna annonser på Google ökat markant. Google varnade för förändrade strategier angående annonsbluffar i mars 2021 och ämnet blev även en relevant diskussion i Sverige. Utöver traditionellt malware som tar över din dator är många av dagens annonsbluffar relaterade till exempel till bitcoin. Efter att du klickat på en elakartad annons som uppmanar dig att köpa bitcoin förs du vidare till sidor där du ska uppge dina bankuppgifter. Eftersom det är fråga om adware får bedragarna enkelt tillgång till din sekretessbelagda information och kan utnyttja den till exempel till att stjäla pengar.

Kryptovalutor är inte det enda ämnet som annonsbluffar och malware drar nytta av. Den skadliga programvaran kan vara relaterad till vad som helst för aktuellt ämne och därför ska du inte surfa på nätet eller klicka på mystiska länkar utan relevant antivirusskydd.

Social engineering, på svenska även känt som social ingenjörskonst eller social manipulation, innebär att lura eller manipulera oskyldiga användare på nätet. Begreppet är brett och omfattar olika tekniker som bedragare använder för att lura åt sig personuppgifter, pengar eller inloggningsuppgifter online. Kärnan i social ingenjörskonst ligger i utnyttjandet av människors goda avsikter och mänskliga fel. Social engineering-attacker baserar sig därmed på mänsklig interaktion och en framgångsrik attack kräver förståelse för mänsklig psykologi.

Både privatpersoner och företag är lika lockande måltavlor för manipulation och lurande. De anställda i stora företag kan ofta bli offer för för social manipulation eftersom bedragare vill få tag på konfidentiell affärsinformation, datorsystem eller andra värdefulla tillgångar. Bara ett litet mänskligt misstag behövs för att utsätta hela organisationer för social engineering-attacker och därför är utbildning av anställda samt skolning om cybersäkerhet viktigt.

Hur fungerar en social engineering-attack?

Många social engineering-attacker följer ett liknande mönster:

1. Identifiering av offret samt insamling av information om hen.
2. Att närma sig offret med falsk identitet och ett påhittat scenario.
3. Efter att ha fått offrets förtroende utförs attacken och manipulationen.
4. Slutförning av attacken och förstörelse av spår som kan leda till att åka fast.

Målet med attacken och manipulationen är att få tillgång till konfidentiell information, vägleda offret till skadliga webbsidor, lura hen till att ladda ner ett virus eller skicka över pengar till bedragaren. Vissa attacker utförs även för att få tillgång till en fysisk enhet eller till exempel ett företags utrymmen. För att få offren att göra som bedragarna vill påstår de sig vara personer eller institutioner som offren litar på, till exempel deras förmän, någon statlig enhet eller en nära vän.

Social ingenjörskonst baserar sig ofta på en känsla av brådska för att offret inte ska ha tid att tänka rationellt. De kriminella är skickliga på att hota eller utpressa offer. Attackerna är ofta utförligt planerade och kan riktas till flera personer samtidigt.

Eftersom alla typer av social engineering bygger på att människor beter sig på ett förutsägbart sätt eller följer ett visst mönster, har attackerna börjat kallas för human hacking, på svenska mänsklig hackning eller mänskliga dataintrång. Genom att dra i rätt trådar kan onlinebrottslingar och bedragare få sina offer att göra saker som många skulle anse väldigt osannolika — tills de själva blir offer.

Hur kan social engineering-attacker förhundras?

Eftersom social engineering baserar sig på mänskliga misstag kan attackerna inte förhindras enbart genom att fixa fel i mjukvaror eller digitala program. Som tur kan både privata konsumenter och företag göra mycket för att stoppa attackerna:

- Använd tvåfaktorsautentisering för att skydda användarkonton.
- Klicka aldrig på misstänkta länkar och ladda inte ned underliga filer.
- Försäkra dig om mottagarens identitet innan du ger ut konfidentiell information.
- Dela aldrig dina inloggningsuppgifter, såsom lösenord eller bekräftelsekoder.
- Anslut inte fysiska externa enheter, till exempel USB-minnen, till din enhet om du är osäker på deras ursprung.
- Ställ dig källkritiskt mot oväntade erbjudanden, speciellt om de verkar för bra för att vara sanna.
- Om det finns barn i ditt hushåll, lär dem vad informationssäkerhet innebär och hur de ska agera på internet.
- Var försiktig med vad du avslöjar på sociala medier eftersom dina konton kan användas som informationskällor för att manipulera dig.
- Skydda dina enheter med pålitliga och heltäckande onlineskydd, till exempel anti-virusprogram och brandväggar.
- Använd en säker VPN när du använder allmänna Wi-Fi-nätverk.
- Begränsa administrationsrättigheter för att kontrollera vem som kan ändra nätverks-inställningar eller installera nya program. Detta är ett sätt att förhindra att användare installerar skadlig programvara på egna eller företagets enheter.

Olika typer av social engineering

Metoderna och teknikerna för manipulation skräddarsys utifrån angriparens mål och syfte. Förståelse för hur de olika teknikerna fungerar är en förutsättning för att kunna identifiera och skydda sig mot social engineering-attacker.

Nätfiske — phishing

En av de vanligaste typerna av social engineering är nätfiske eller så kallat phishing. Nätfisket går ut på att lura offret till att ange personlig eller ekonomisk information som kan utnyttjas i attacken. Målet kan också vara att offret ska ladda ner en fil eller en programvara som är infekterad med virus eller malware. Även om phishing ofta sker genom e-postmeddelanden finns det också andra metoder för att utföra det.

- **Vishing**: Termen vishing är en sammansättning av de engelska orden voice och phishing. Onlinekriminella försöker få tag på värdefull information genom röst-baserade metoder, så som telefonsamtal. Till exempel många kärleks- och romansbedrägerier sker via telefonsamtal. Bedragaren charmar offret på telefon men är i verkligheten bara ute efter pengar som offret lätt skickar till sin förmodade nyfunna kärlek.
- **Smishing**: Att använda SMS och snabbmeddelandetjänster för att lura folk kallas för smishing. De flesta telefoner är idag kopplade till internet och därför kan phishingmeddelanden som skickas via textmeddelanden lätt innehålla länkar som leder användaren till skadliga webbsidor.
- **Spear phishing**: Social engineering-attacker riktas ofta mot många offer samtidigt, men konceptet spear phishing syftar på en cyberattack där en särskild måltavla väljs. Meddelandena som skickas i samband med spear phishing är anpassade för det specifika offret och är därför svåra att identifiera. Angriparen kan till exempel påstå sig vara VD för ett företag i syfte att lura de anställda. Bedragaren utnyttjar då en betrodd persons auktoritet för att vinna offrets förtroende.

Pretexting

Den dimension av social engineering som kallas pretexting innebär att angriparen ljuger om en situation, eller en så kallad pretext, för att lura offret till att uppge sekretessbelagd information eller utföra vissa handlingar. Bedragaren påstår sig vara en representant från någon myndighet, offrets medarbetare eller någon annan person som offret litar på. När bedragaren fått offrets förtroende kan hen lätt få hen att avslöja konfidentiell information, klicka på en infekterad länk eller skicka pengar. Kärnan i pretexting ligger i att skapa en övertygande historia som inte väcker några misstankar hos offret.

Baiting

Baiting omfattar någon typs fysiskt medium, till exempel en USB-sticka eller en CD-skiva, som infekterar en enhet med malware eller virus. Bedragare kan till exempel lämna dessa mystiska medier på allmänna platser eller i ett företags utrymmen. Metoden baserar sig på människans nyfikenhet som kan stimuleras ytterligare genom frestande etiketter och märken på mediet.

Att läsa USB eller DVD skiva i datorn

För att undkomma att felaktigt/skadande filer kommer in i företagets datormiljö är det rekommenderat att ha en fristående dator med uppdaterat virusskydd som man kontrollerar skivan eller USB minnet på.

Detta sker genom att man först uppdaterar virusskyddet på datorn genom att koppla in den på nätverket, välj uppdatera Antiviruset om den inte gör detta själv.

Koppla ur nätverkskabeln ur datorn.

Därefter stoppa in eller sätt i USB minnet, högerklicka på enheten och välj scanna enhet.

Finns det virus på enheten varnar programmet är där inga virus säger den OK, då kan man flytta över infon till en dator och läsa in filerna.

Har man möjlighet att sätta in en bättre brandvägg i sitt nätverk, kan denna dator få en egen utgång till Internet och på det sättet hålla sig uppdaterad, men inte påverka övriga datorer på nätverket.
Denna brandvägg kan även ställas in så att känsliga datorer inte når Internet, detta krävs oftast för ett Ransomware som krypterar datorerna ska kunna aktivera sig.

Hur ska man att se över sin utrustning på kliniken och övertyga chefen

- Var tydlig med att det är dags att uppdatera viss utrustning samt att ni har en kontakt som kan hjälpa er att plocka fram rätt produkter
- Att tidigare inköp av utrustning inte höll måttet, samt att ni kan få ett förslag på hur man kan finansiera istället för att köpa kontant
- Att personalen är en del i beslutsprocessen för det som ska köpas in och det behöver tas upp till diskussion.
- Att ni vill bjuda in en extern IT-konsult som kan berätta om möjligheterna till förbättringar
- Skaffa samma utrustning va det gäller datorer och skärmar så alla känner igen sig.

Backup av servrar och information

Om ni tar backup på era servrar och information är det viktigt att ha flera medier som man växlar mellan, tagen backup ska aldrig förvaras på kliniken, detta om det skulle brinna eller bli inbrott, ta backupen och plocka med er disken hem, rekommenderat är minst 3 diskar för backup, 2 som man växlar mellan dagligen och 1 som är en månadsbackup.

Tar er leverantör backupen till er säkerställ med dessa vilka skydd de har för att inte kunna skicka in skadlig kod via deras ”tunnel” som är kopplad till er verksamhet, samt vilka skydd de har på sin utrustning.

Om ert system är molnbaserat

Om ni använder ett molnbaserat journalsystem kontrollera med er leverantör vad de har för skydd på sin utrustning mot skadlig kod, lägger deras system ned då har ni ingen möjlighet att nå era journaler, som ett exempel råkade Coop ut för detta ifjor då alla butiker stod stilla, det var deras leverantör i USA som hade drabbats.

Tips på program att kolla på är tex

- TV serien Hackad på SVT Play, Linus Kvarnhammar i programmet är en samarbetspartner till mig, här ser ni hur det kan gå till när de kommer över information från era enheter, bla från Kristoffer Appleqvist från Svenska Nyheter där de hackar hans privata konto.

Vill ni ha ytterligare hjälp med er verksamhet erbjuder jag följande

- Ta fram policys
- Offerter på lämplig utrustning skärmar, datorer och tillbehör
- Ergonomiska produkter, stolar, bord, mattor
- Skrivare
- Skyddsutrustning till röntgenrum, till personal mm
- Backuplösningar
- Brandväggar
- Hotutbildning = lära sig hitta hoten som kommer i mail, länkar mm

Om det är något annat som ni funderar över går det att nå mig på min mailadress joacim@ctrl-alt.se eller 0733-932300 om ni vill prata istället.

Mvh

Joacim Mårtensson