TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Anvisning – Läckta användarkoder

Traficoms publikationer
22/2022

Innehållsförteckning

1 Inledning

1.1 Syftet med anvisningen

Denna anvisning har utarbetats av Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom och syftar till att ge organisationer råd i situationer, där man misstänker att användarkoder har läckt ut till obehöriga personer eller aktörer och att de har utnyttjats i ett cyberangrepp. Fokus för anvisningen ligger på att behandla särdragen för denna typ av informationssäkerhetsincident. För att lösa situationen i sin helhet är det bra om organisationen upprätthåller och följer den incidenthanteringsplan som den upprättat för informationssäkerhetsincidenter (eng. Incident Response Plan).

Denna anvisning ger övergripande vägledning för hur man ska agera vid informationssäkerhetsincidenter och hur man kan återhämta sig från dem. Det rekommenderas att organisationen upprättar en egen separat guide, som på en mer detaljerad nivå beaktar organisationens tekniska och operativa miljö. Projektet har finansierats av Försörjningsberedskapscentralen.

1.2 Vad betyder läckta användarkoder?

Läckta användarkoder är ett av de vanligaste sätten för angripare att ta sig in i din organisations informationssystem. Läckta användarkoder används många gånger för att få det första fotfästet vid angrepp. Användarkoder köps och säljs på handelsplatser som används av kriminella samt delas offentligt i form av stora databaser.

Koderna hamnar oftast i fel händer till följd av ett dataläckage hos en tredje part, på grund av att lösenord återanvänds eller med hjälp av nätfiskemeddelanden. Det är av största betydelse att din organisations lösenordspraxis är uppdaterade och att personalen utbildas för att minimera riskerna.

1.2.1 Vd-bedrägeri

Vid ett vd-bedrägeri (eng. Business Email Compromise) luras en anställd som har hand om företagets penningrörelse att betala en faktura eller göra någon annan kontoöverföring med företagets medel till ett konto som innehas av kriminella. På svarta marknaden köper nätbrottslingar användarkoder, som de kan använda för att logga in till den anställdas e-post och följa e-posttrafiken för att leta efter till exempel möjligheter att göra ändringar i innehållet, till exempel kontonummer, i befintliga meddelandekedjor. De kan även skapa helt nya fakturor och styra betalningarna av dem till sina egna konton.

2 Beredskap

Ett bra sätt att minska incidenternas allvarlighetsgrad samt möjliggöra snabb återhämtning och att affärsverksamheten kan fortsätta är att förbereda sig för incidenter. Organisationen kan bedöma sin beredskap genom att använda till exempel Cybersäkerhetscentrets Cybermätare[1]. En i förväg upprättad incidenthanteringsplan ger ett bra utgångsläge för hur man ska agera när en incident inträffar. Organisationen ska även säkerställa att olika åtgärder, till exempel att låsa användarkoder, blockera servrar och enheter från nätet samt begränsa nättrafiken till skadliga IP-adresser eller domännamn, är tekniskt möjliga och att personalen även har kompetens för att genomföra dem.

Det är viktigt att samla in, sammanställa och övervaka loggdata för att kunna upptäcka incidenter i tid. Loggdata gör det även möjligt att utreda incidenter grundligt och på så sätt göra den eventuella rensningen och återställandet av miljön snabbare. Cybersäkerhetscentret har utarbetat anvisningar för hur man samlar in och använder loggdata.[2] Beroende på vilka system en organisation använder, krävs vanligtvis dessutom lösningar på nätverks- och systemnivå för omfattande monitorering.

Företagets allmänna lösenordspolicy, begränsning av inloggningskällor och flerfaktorsautentisering är utmärkta sätt att förhindra att läckta användarkoder utnyttjas.

2.1 Administrativa åtgärder

- Inför en incidenthanteringsplan i vilken ingår tydliga anvisningar för personalen vid incidenter som anknyter till läckage av användarkoder.
- Planera en lösenordspolicy för din organisation, där minimikraven för lösenord definieras.
- Utbilda personalen i att känna igen nätfiskemeddelanden per e-post.
- Ta i förväg reda på hur du kan anmäla en informationssäkerhetsincident till Cybersäkerhetscentret[3]. Följ Cybersäkerhetscentrets aktuella meddelanden.[4]
- Gå igenom olika angreppsscenarier tillsammans med ledningen och kom överens om praktiska åtgärder samt ledningsansvar och -befogenheter vid informationssäkerhetsincidenter.
- Öva på[5] och utveckla incidenthanteringsplanen regelbundet med hjälp av diskussionsbaserade övningar (eng. Tabletop Exercise) , där de ansvariga personerna och intressenterna övar på processen för hantering av informationssäkerhetsincidenter i ett fiktivt scenario.
- Definiera noggrant vilka behörigheter som behövs för användarna och de tekniska funktionerna.
- Överväg att inrätta ett säkerhetsoperationscenter eller att köpa en motsvarande tjänst. Syftet med en sådan säkerhetstjänst är att övervaka ditt företags nättrafik och informationssäkerhetsincidenter i systemen.

[1] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren
[2] https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-har-samlar-du-och-anvander-loggdata
[3] https://www.kyberturvallisuuskeskus.fi/sv/anmal

[4] https://www.kyberturvallisuuskeskus.fi/sv/ajankohtaiset

[5] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/ovningar

2.2 Tekniska åtgärder

- Inför flerfaktorsautentisering.
- Begränsa inloggningsförsöken från länder, där din organisation inte har någon affärsverksamhet.
- Inför identitets- och åtkomsthantering (eng. Identity and Access Management, IAM).
- Genom att använda ett virtuellt privat nätverk (eng. Virtual Private Network, VPN) kan du hindra inloggningsförsök från externa nätverk till de mest kritiska systemen.
- Sträva efter att upptäcka angrepp så tidigt som möjligt med hjälp av olika centraliserade övervakningslösningar och testa deras funktion regelbundet.
- Ta i bruk funktioner i de befintliga systemen eller skaffa en informationssäkerhetsprodukt som kan filtrera e-postmeddelanden med skadligt innehåll samt skräppost och icke önskvärd nättrafik.

2.3 Beredskap och övning i praktiken

En viktig del av beredskapen är även att öva på hotscenarier. Genom att i förväg öva på liknande scenarion som det som beskrivs i denna anvisning kan din organisation säkerställa att den är redo att möta en dylik situation. Genom att öva försäkrar du dig bland annat om att personalen i din organisation förstår vad punkterna i arbetsflödesschemat och checklistan i denna anvisning betyder och att den har förmåga att agera enligt de anvisningar som beskrivs.

Organisationer rekommenderas även ta del av Cybersäkerhetscentrets material om övningar.[6]

Ett exempelscenario skulle kunna vara en situation där användarkoderna för en av företagets anställda har hamnat i händerna på nätbrottslingar. Koderna har använts för att logga in till ett e-postkonto, varifrån falska fakturor har skickats. Informationssäkerhetsincidenten kommer fram när en samarbetspartner upptäcker misstänksamma detaljer i fakturor som den fått.

Hur skulle man i din organisation agera i en dylik situation? Öva på åtminstone följande steg i dessa anvisningar:

- Informera om incidenten och eskalera situationen.
- Lås infekterade koder och bryt aktiva sessioner.
- Samla in identifieringsuppgifter om inloggningshändelser samt logganalys.
    - Kan ni ta reda på hur användarkoderna har läckt ut?
    - Vems användarkoder har blivit utsatta?
- Använd de insamlade identifieringsuppgifterna för att kontrollera om andra användarkoder är infekterade.
- Ta reda på vem som tagit emot nätfiskemeddelandet.
- Genomför en process för den slutliga utredningen av incidenten.

[6] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/ovningar

Vid sidan om alla steg att öva på är det bra att tänka på hur organisationen leder hanteringen av informationssäkerhetsincidenten, hur den interna kommunikationen fungerar samt vem som i vilket skede är ansvariga personer och vem deras ersättare är.

3 Upptäcka en informationssäkerhetsincident

En informationssäkerhetsincident till följd av läckta användarkoder kan upptäckas på till exempel följande sätt:

- Organisationen får ett meddelande om misstänkt aktivitet eller e-post, till exempel via sociala medier, en kund, en samarbetspartner eller en myndighet.
- En informationssäkerhetsprodukt eller en tjänsteleverantör avger ett larm.
- En tjänst för information hot skickar ett meddelande om läckta användarkoder.

Anmäl informationssäkerhetsincidenten till Cybersäkerhetscentret.[7] Vi ger er konfidentiellt och kostnadsfritt råd för hur ni begränsar skadorna, analyserar incidenten och vidtar återställande åtgärder. Samtidigt stöder ni den nationella lägesbilden av informationssäkerheten och gör det möjligt för oss att varna och hjälpa andra eventuella offer.

Läs Cybersäkerhetscentrets anvisning för hur man upptäcker dataintrång (på finska).[8]

[7] https://www.kyberturvallisuuskeskus.fi/sv/anmal

[8] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

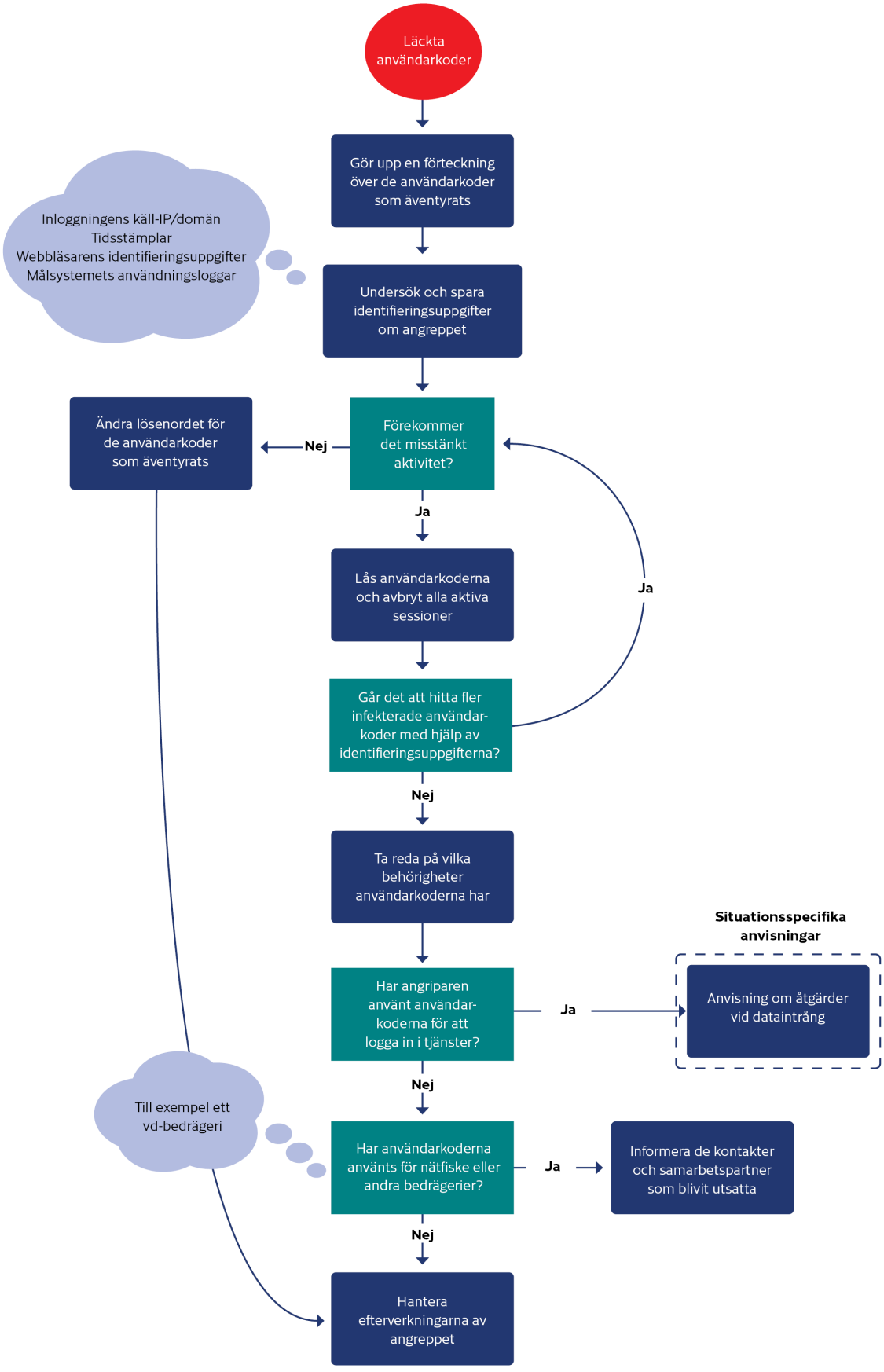
4 Anvisningar

Använd nedanstående checklista på åtgärder som hjälp när du upptäcker en informationssäkerhetsincident som berör användarkoder. Checklistan hjälper organisationen att prioritera och dela in verksamheten vid utredningen av en incident.

4.1 Arbetsflödet vid utredning av en informationssäkerhetsincident

Nedanstående flödesplan beskriver de åtgärder som ska tillämpas för att en incident ska kunna utredas i rätt ordning. Flödesplanen stöder användningen av checklistan. Under utredningen är det även ytterst viktigt att föra en noggrann händelselogg över de åtgärder som vidtagits. Av loggen ska framgå vilken åtgärd som genomförts, tidsstämpeln för den och vem som utfört åtgärden.

Det är även skäl att omsorgsfullt dokumentera eventuellt bevismaterial. Det bör antecknas vem som samlat in materialet, vad materialet består av samt var och när det har samlats in. En omsorgsfullt upprättad händelselogg underlättar avsevärt utredningen samt samarbetet med polisen och datasäkerhetsforskarna.


Läckta användarkoder
Gör upp en förteckning över de användarkoder som äventyrats
Inloggningens käll-IP/domän
Tidsstämplar
Webbläsarens identifieringsuppgifter
Målsystemets användningsloggar
Undersök och spara identifieringsuppgifter om angreppet
Förekommer det misstänkt aktivitet?
Nej
Ändra lösenordet för de användarkoder som äventyrats
Ja
Lås användarkoderna och avbryt alla aktiva sessioner
Ja
Går det att hitta fler infekterade användar-koder med hjälp av identifieringsuppgifterna?
Nej
Ta reda på vilka behörigheter användarkoderna har
Situationsspecifika anvisningar
Har angriparen använt användar-koderna för att logga in i tjänster?
Ja
Anvisning om åtgärder vid dataintrång
Nej
Till exempel ett vd-bedrägeri
Har användarkoderna använts för nätfiske eller andra bedrägerier?
Ja
Informera de kontakter och samarbetspartner som blivit utsatta
Nej
Hantera efterverkningarna av angreppet

4.2 Omedelbara åtgärder

Stegets mål	Det är viktigt att åtgärderna är både exakta och snabba. Målet med de omedelbara åtgärderna är att stoppa spridningen av den skadliga programvaran, hindra angriparna från att få fotfäste i nätverket och förbereda inledningen av återhämtningsprocessen.

Steg	Syfte	Åtgärder
Lås användarkoden	Genom att låsa användarkoden och avbryta aktiva sessioner förhindrar man att användarkoderna missbrukas.	Lås användarkoden på ett sådant sätt att den inte kan användas. Avbryt alla aktiva sessioner.
Ta reda på behörigheterna för användarkoderna	Beroende på behörigheterna för användarkoderna kan de missbrukas på olika sätt. Sök svar på följande frågor: • Vilka system kan man logga in i med användarkoderna? • Har koderna administratörsbehörigheter till systemen eller andra användarkoder?	Ta reda på behörigheterna för användarkoderna.
Bedöm om du behöver utomstående hjälp för att hantera informationssäkerhetsincidenten	Organisationen kan behöva hjälp med att organisera åtgärder, hantera incidenten och utföra tekniska åtgärder. Om det inte finns tillräcklig kompetens i den egna organisationen eller hos IT-tjänsteleverantören ska man överväga att anlita hjälp utifrån.	De tekniska åtgärderna vid hanteringen av en incident kan kräva extern kompetens. Sådana åtgärder kan vara bland annat insamling av identifieringsuppgifter och utredning av hotet utifrån dem. Cybersäkerhetscentret kan hjälpa organisationer med i synnerhet de första insatserna och genom att erbjuda tilläggsinformation om liknande fall i Finland och internationellt. I resurserna i fotnoten hittar du finländska tjänsteleverantörer.[9]
Rapportera informationssäkerhetsincidenten till myndigheterna	Rapportera incidenten till myndigheterna. Organisationen kan enligt författningar eller villkoren i cyberförsäkringen vara skyldig att anmäla informationssäkerhetsincidenten.	Gör en brottsanmälan om händelsen till polisen.[10] Anmäl händelsen även till Cybersäkerhetscentret[11] för att upprätthålla lägesbilden och få hjälp. Om det är möjligt att personuppgifter eller andra uppgifter som omfattas av dataskyddslagstiftningen (GDPR) har hamnat i händerna på angriparen, gör en anmälan till dataombudsmannens byrå[12]. Aktörer och tjänsteleverantörer, som är kritiska med tanke på försörjningsberedskapen och som omfattas av EU:s direktiv

[9] https://dfir.fi/
https://www.fisc.fi/fi
https://www.hansel.fi/sv/upphandlingar/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/

[10] https://poliisi.fi/sv/gor-en-brottsanmalan

[11] https://www.kyberturvallisuuskeskus.fi/sv/anmal

[12] https://tietosuoja.fi/sv/anmalan-om-personuppgiftsincident

		om säkerhet i nätverks- och informationssystem (s.k. NIS-direktivet), ska anmäla informationssäkerhetsincidenter i nätverks- och informationssystem till tillsynsmyndigheterna[13].

[13] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/rapportera-en-it-sakerhetsincident-nis-skyldighet

4.3 Utredning av en informationssäkerhetsincident

Stegets mål	Målet med utredningen av incidenten är att ta reda på angreppets omfattning och effekt i organisationen. Genom en omsorgsfull utredning säkerställs att angriparen inte längre har tillträde till systemen och att man åter har kontroll över alla utsatta användarkoder.

Steg	Syfte	Åtgärder
Identifiera skadlig aktivitet och samla in identifieringsuppgifter	Identifieringsuppgifter används för att kartlägga vilka enheter och användarkoder som är infekterade. Att omsorgsfullt samla in identifieringsuppgifter och använda dem vid utredningen av incidenten är livsviktigt för att miljön ska kunna rensas tillräckligt väl, så att återställandet kan inledas på ett säkert sätt.	Leta efter avvikelser i de loggdata som är tillgängliga för att upptäcka huruvida de läckta användarkoderna har utnyttjats. Avvikelser kan vara till exempel: • inloggningstidpunkten • käll-IP-adressen • operativsystemets eller webbläsarens version. Bekräfta observationerna genom att intervjua användarkodernas ägare för att försäkra dig om att åtgärderna inte har utförts av honom eller henne. Spara identifieringsuppgifterna om avvikelserna som du kan använda för att leta efter andra användarkoder, vars uppgifter eventuellt har läckt ut.
Använd identifieringsuppgifterna för att hitta samtliga läckta användarkoder	Med hjälp av de insamlade identifieringsuppgifterna kan man ta reda på i hur stor omfattning angriparen har tagit sig in i organisationen. Genom att samla in identifieringsuppgifter och söka dem i målsystemen kan man försäkra sig om att alla infekterade enheter och koder hittas och åtgärdas.	Med hjälp av centraliserade övervakningsprogram kan man leta efter läckta användarkoder. Programmen erbjuder ofta en möjlighet att söka händelser på alla enheter med de önskade användarkoderna. Om organisationen även har en centraliserad logghantering kan man med hjälp av den effektivt söka händelser i flera olika källor samtidigt. Om ingen av de ovanstående lösningarna är tillgängliga ska identifikationskoderna sökas manuellt på alla enheter och servrar. Det finns en risk att angriparen, efter att ha tagit sig in i en enhet, har kopplat bort insamlingen av loggar, vilket innebär att det inte finns några spår efter hans eller hennes aktivitet. Därför är det viktigt att undersöka identifieringsuppgifterna som samlats in från alla de olika källorna och med hjälp av dem försöka skapa sig en helhetsbild av angriparens aktivitet.
Spara alla tillgängliga loggfiler och övriga bevis på en hårddisk som är isolerad från nätverket för senare undersökning	Syftet med att samla in och spara bevis är att säkerställa en högklassig utredning av incidenten i efterhand, så att grundorsakerna till den kan klarläggas. Bevisen kan behövas i samband med en brottsanmälan och för rättegångsförhandlingar.	Spara de loggfiler som innehåller viktig information med tanke på undersökningen av incidenten på en hårddisk som är isolerad från nätverket. Samla även in eventuella skadliga e-postmeddelanden och övriga meddelanden.

	Om organisationen har en cyberförsäkring kan även försäkringsbolaget kräva närmare uppgifter om incidenten samt bevis för en utredning.	Sträva efter att förvara bevisen, såsom kompletta skivavbilder och minnesprover, så enhetliga som möjligt. Använd en hashfunktion för att säkerställa deras integritet. Försök ta prover av de skadliga programvarorna och spara dem. Särskild försiktighet ska iakttas vid hanteringen. En säker förvaring kräver ofta yrkeskompetens. Skicka proverna till Cybersäkerhetscentret.[14]
Intervjua användaren	Bekräfta observationerna genom att intervjua den användare som äger de läckta användarkoderna. Användaren kan eventuellt ge information om hur koderna har läckt ut. Användaren kan ha till exempel laddat ner filer till sin dator, klickat på en länk i ett e-postmeddelande eller öppnat en fjärranslutning för en angripare, som utgett sig för att vara IT-stödperson. När användaren intervjuas ska han eller hon inte skuldbeläggas för det inträffade, eftersom hans eller hennes handlingar inte nödvändigtvis har något att göra med att uppgifterna läckt ut och användaren märkte inte nödvändigtvis att något avvikande skett.	Intervjua användaren, vars användarkoder använts för ovanlig aktivitet, och försök reda ut orsakerna till att koderna läckt ut.

[14] https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/formedla-e-post-och-prov-till-cybersakerhetscentret

4.4 Återställande

Stegets mål	Målet är att återta kontrollen över samtliga läckta användarkoder och säkerställa att koderna återigen är säkra. Verksamhetsmodellerna förbättras, så att liknande händelser kan undvikas framöver.

Steg	Syfte	Åtgärder
Ändra lösenordet för användarkoderna	Se till att inloggningsuppgifterna för samtliga infekterade användarkoder ändras, så att angriparen inte längre har tillträde till organisationens system med hjälp av koderna.	Ändra lösenordet och be användaren att ändra lösenordet på nytt när han eller hon loggar in första gången. Informera användarna om de nya lösenorden antingen muntligt, per sms eller per telefon, men använd inte e-post eller de snabbmeddelanden som organisationen använder, eftersom angriparen fortfarande kan ha tillträde till dem. Överväg att införa tvåfaktorsautentisering för administratörskoderna och de koder som utnyttjades under angreppet. Övervaka även de koder som användes vid angreppet noggrannare efter att de återställts, för den händelse att angriparen på nytt kommer över dem. Om det förblir oklart hur angriparen kunde komma över vissa koder, överväg att förstöra dem och skapa helt nya koder. På så sätt försäkrar du dig om att angriparen inte kommer över koderna på nytt på samma sätt. Överväg även att ge ägaren av de läckta användarkoderna en ny arbetsstation.
Kontrollera reglerna för omdirigering av e-postmeddelanden	Vid vd-bedrägerier ställer man ofta in omdirigeringsregler för e-postkonton, med hjälp av vilka brottslingarna kan följa organisationens e-posttrafik.	Kontrollera omdirigeringsreglerna för de läckta användarkodernas e-postkonton och ta bort de skadliga regler som du upptäcker.
Skärp inloggningskraven för användarna	Man kan begränsa missbruk av de läckta användarkoderna genom att skärpa inloggningskraven.	Sätt inloggningskraven på en lämplig nivå genom att införa följande skärpningar: • flerfaktorsautentisering • certifikatbaserad inloggning • domänanslutna enheter eller enheter som företaget kontrollerar på annat sätt • begränsning på basis av käll-IP-adress.
Utvärdera nuvarande lösenordspraxis	Genom att upprätthålla en lösenordspraxis fastställs minimikraven för lösenordens komplexitet.	Utvärdera och uppdatera anvisningarna för lösenordspraxisen.

5 Efterverkningar av informationssäkerhetsincidenten

När krisen är över och affärsfunktionerna normaliserat sig är det viktigt att börja hantera efterverkningarna av angreppet och lära sig av det inträffade för framtiden. Samtidigt är det skäl att uppdatera krishanteringsplanerna utifrån de observationer som gjorts. Det är möjligt att organisationen på nytt faller offer för ett liknande angrepp om grundorsakerna till det inträffade inte kommer fram och man inte tar lärdom av händelsen.

Vid hanteringen av efterverkningarna (eng. Post-Incident Review) granskas verksamheten i krissituationen: vilka åtgärder genomfördes väl, var fanns det utrymme för förbättringar samt hur kan säkerhetsnivån och -planerna förbättras? Det är skäl att utarbeta en rapport om hanteringen av efterverkningarna som, förutom händelseförloppet, även inkluderar svar på åtminstone följande frågor:

- Grundorsaker till incidenten:
    - Vilka tekniska eller funktionsmässiga svagheter ledde till situationen?
- Det egna skyddets effektivitet:
    - Var de kontroller som användes för att upptäcka angrepp tillräckliga?
    - Orsakade angriparens handlingar några larm?
    - Hur reagerade man på larmen? Fick rätt ansvariga personer information om larmen?
- Agerande i krissituationen:
    - Följde man krisplanen? Hur användbar var den?
    - Fördelades krisgruppens ansvar mellan rätt personer?
    - Hur väl lyckades man begränsa angreppet och driva bort angriparen?
    - Hur väl lyckades krisgruppens kommunikation? Hur beaktades intressenterna?
- Återställande:
    - Hur väl lyckades man återställa kritiska uppgifter och tjänster?
- Efterverkningar:
    - Har händelseförloppet och utredningsarbetet dokumenterats?
    - Var den tekniska utredningen av incidenten tillräcklig? Har man kunnat förse till exempel myndigheterna med tillräckligt med material om angreppet?
    - Utvärdera tjänsteleverantörernas verksamhet. Var svarstiden och de avtalade tjänsterna tillräckliga för att utreda incidenten?

Efter incidenten ska organisationen uppdatera sin incidenthanteringsplan och sina mer detaljerade anvisningar för bekämpning av olika typer av avvikelser. Det rekommenderas även att organisationerna med jämna mellanrum övar på olika scenarier, så att nyttan med dem kan garanteras vid en krissituation.

Cybersäkerhetscentret önskar att företag och organisationer skulle dela med sig av de viktigaste lärdomarna som de dragit av incidenter. Med hjälp av fallrapporter kan Cybersäkerhetscentret hjälpa andra organisationer i Finland och utomlands vid utredningen av liknande fall. De lärdomar som återställandet ger bidrar till att utveckla beredskapen för alla organisationer.

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret
PB 320, 00059 TRAFICOM
tfn 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-814-0

FÖRSÖRJNINGS-
BEREDSKAPCENTRALEN

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret