Ert datum	Er referens
2013-10-28	131 647171 - 13/111
	131 647173 - 13/111
	131 647177 - 13/111
Datum	Vår referens
2014-02-03	NW/EÖ

IT&Telekomföretagen
almega

Urban Bjergert
Skatteverket
Huvudkontoret
Rättsavdelningen
Box 10
221 00 Lund

Yttrande avseende Skatteverkets förslag till föreskrifter om kontrollsystem till kassaregister, krav på kassaregister och användning av kassaregister

Kassaregisterrådet under IT&Telekomföretagen har erbjudits möjlighet att inkomma med synpunkter på rubricerade förslag.

Vi tackar för möjligheten och vill framföra följande.

Sammanfattning

Idag tillåts inte att köp genomförs om inte kassaregistret har kontakt med en kontrollenhet. Om kontrollenheten är placerad så att den nås över internet uppstår problem vid avbrott på förbindelsen. Förslaget föreslår en lösning på detta genom att buffring av dataöverföringen mellan kassaregistret och kontrollenheten tillåts. Dessutom innehåller förslaget ett antal olika konfigurationer som ska möta önskemål om att använda både fysiska och virtuella datorer och olika typer av kassaregister.

Kassaregisterrådet instämmer i att det finns ett behov av att tillåta buffring för att kunna erbjuda serverbaserade kontrollenheter och uppskattar att Skatteverket utarbetar förslag till lösningar.

Den lösning som föreslås är dock mycket komplicerad. Kontrollenheten består av buffringsprogram, signeringsmodul och kontrollserver. Proceduren för att konfigurera och använda systemet innehåller mycket komplex hantering av bland annat skapande av nycklar, kryptering, informationsöverföring, aktivitets-kontroller samt omfattande processer för att kunna kontrollera och hämta ut lagrad information. Dessutom är kraven på kontrollservern omfattande med certifiering av ackrediterat certifieringsorgan samt att den miljö som servern ska vara placerad i har långtgående krav, t.ex. avseende loggar, både manuella och automatiska, uthämtning av data, bevarande av data samt diverse regelbundet återkommande kontroller av olika karaktär.

I och med lösningens komplexitet inställer sig frågan vilken marknad som kommer att använda systemet och, inte minst, vilka tillverkare och leverantörer som kommer att erbjuda det.

Kassaregisterrådet befarar att förslaget på ett alltför komplext sätt försöker erbjuda en lösning på buffringsproblemet vilket gör att få eller kanske ingen ser en affärsnytta i att välja lösningen.

En annan aspekt är att förslaget inte möter det som egentligen är en av de primära drivkrafterna bakom serverbaserade kontrollenheter med möjlighet till buffring vilket är kassor i mobiler, plattor eller likande.

Rekommendation

Kassaregisterrådet rekommenderar därför att förslaget omarbetas till en mindre komplex lösning som även tillgodoser användningen av mobila kassor.

Vidare arbete

Kassaregisterrådet föreslår, oberoende av hur det lagda förslaget kommer att hanteras, att det snarast inrättas en arbetsgrupp mellan Skatteverket och branschen. Dess uppgift är att på *huvudkravsnivå* identifiera lösningar för buffringsproblemet samt specifikt för serverbaserade kontrollenheter för mobila kassor.

Svarets struktur

Beroende på att Kassaregisterrådet i princip anser att förslaget bör omarbetas så kan detaljerade kommentarer på det befintliga anses överflödiga eller tolkas som ett accepterande av förslagets omfattning, upplägg och komplexitetsnivå. Dock anser Kassaregisterrådet att det som nedan kommenteras kan tjäna som underlag till vidare arbete.

Med vänliga hälsningar

Thor Johnsson

Ordförande Kassaregisterrådet

Nils Weidstam

Nils Weidstam

Näringspolitisk expert

Ellinor Bjennbacke

Ellinor Bjennbacke

Näringspolitisk chef för IT&Telekomföretagen

Allmänt

Förslaget SKVFS 2013:X har tagits fram för att utgöra ett alternativ till kontrollenheter enligt Skatteverkets föreskrifter SKVFS 2009:2 om kontrollenhet till kassaregister Förslaget SKVFS 2013:Y och SKVFS 2013:Z har tillkommit främst som en följd av förslaget om kontrollsystem till kassaregister.

Förslaget SKVFS 2013:Y och SKVFS 2013:Z innebär samtidigt förslag till upphävande av Skatteverkets föreskrifter SKVFS 2009:1 om krav på kassaregister och Skatteverkets föreskrifter SKVFS:3 om användning av kassaregister.

Kassaregisterrådet har inget att anföra mot dessa förändringar.

Kommentarer till SKVFS 2013:Y, Krav på kassaregister

5 kap. 1 §

Utökade krav på registrering och förändring av växelkassa. Här behöver övergångstiden specificeras.

6 kap. 2 § och 2 kap. 3 §

Det behöver förtydligas att det går att visa kvittodata på skärm men att detta inte är kvittot.

Kommentarer till SKVFS 2013:Z, Användning av kassaregister

4 kap. 1 §

Utökade krav på registrering och förändring av växelkassa. Här behöver övergångstiden specificeras.

4 kap. 3 §

Stängning av kassalådan omedelbart efter försäljning. Är detta ett realistiskt krav?

Kommentarer till SKVFS 2013:X, Kontrollsystem till kassaregister

Kommentarer sidan 3: Definition av kvittokontrolldata saknas.

Kommentarer sidan 5: Lite otydligt vad kvittokontrolldata är.

Kommentarer sidan 5: ” Viss stödinformation” är inte definierat.

Kommentar sidan 6: ”Kontrollsystem” är inte definierat.

Kommentar sidan 6: Kontrollsystemet verifierar löpande sammankopplade enheter. Dessa verifieringar loggas i systemet. Detta skapar ytterligare en komplicerad lagring.

Kommentar sidan 6: Kontrollserverns ska löpande skicka avstämningskoder till buffringsprogrammet. Avstämningskoderna genereras av kontrollservern och för

varje sammankopplat kassaregisternummer. Buffringsprogrammet skickar avstämningskoderna vidare till varje kassaregister. Avstämningskoderna baseras på kvittodata som krypteras med Skatteverkets huvudnyckel.

- Var lagras dessa avstämningskoder
- Denna mottagning måste vara en ny funktion i kassaregister

Kommentar sidan 6: Alla möjligheter att förvara journalminnet? Tillhör inte journalminnet kassaregistret?

Kommentar sidan 7: Om en dator ska användas för flera företag krävs en signeringsmodul på separat programvara per företag. Är detta realistiskt med tanke på att det blir många externa portar som ska kommunicera. Hur vet kassaregistret vilken signeringsmodul som ska användas?

Kommentar sidan 8: Ska det vara TPM-chip, dvs. Trusted Platform Module.

Kommentar sidan 10: Varför ska buffringsprogrammet och signeringsmodulerna befinna sig i samma lokal som kassaregistret? Hur definieras "samma lokal"?

Kommentar sidan 10: Endast en (1) signeringsnyckel per signeringsmodul. Avses här att endast ett (1) organisationsnummer som kan använda lösningarna. Signeringsnyckeln skapas ju av organisationsnummer och kassaregisterprogram. Varför ska alternativ 4 ha en signeringsnyckel per tunn klient? Kassaregisterprogrammet är ju gemensamt.

Kommentar sidan 11: Krävs även här att utrustningen ska stå i samma lokal? (Vad är annars logiken i kravet enligt figur 3)

Kommentar sidan 12, stycke 4.5: Varför ska datorerna med kassaregisterprogram och den dedikerade datorn finnas i samma lokal. Hur definieras lokal?

SKVFS 2013:X

3 kap. Definitioner

27 §

Varför begränsning till två virtuella datorer i definitioner. Jmf. 26§.

4 kap. Hårdvara och programvara för buffringsprogram och signeringsmodul

Fel i paragrafnumreringen fram till 8 §.

46 § (borde varit 7 §)

Reparation får endast utföras av tillverkare av kontrollsystemet eller av denna utsedd behörig reparatör.

- Här borde även återförsäljare läggas till. Tillverkaren kan vara ett företag utanför Sverige.

Tillverkaren ska föra ett register över de reparationer som gjort av virtuella miljöer.

- Tillverkaren kan vara ett stort företag i främmande land. Kravet verkar orealistiskt. Om detta krav ska finnas borde det ligga på den svenska återförsäljaren.
- Kravet blir generellt konkurrensbegränsande med tanke på möjligheten för mindre leverantörer att möte kraven på reparationsverkstäder som kommer att finnas över hela Sverige
- Tillförande av betungande administrativa rutiner förefaller inte fullt proportionerliga.
- Kraven på registerhållning bör tas bort samt även kraven på att endast tillverkaren kan utse behöriga reparationsverkstäder.

8 § p. 1 - 8

Kontrollera rimligheten i kraven. Om detta inte är standardkrav på virtuella datorer bör de anpassas till standardkrav. Det finns inte heller angivet den begränsning om antalet virtuella datorer som gavs i 3 kap. 28 §.

10 §

Återförsäljaren bör kunna infoga signaturen i TPM-chipet av de skäl som redovisas ovan.

14 §

Även här bör återförsäljare tillåtas att reparera en dedikerad dator.

5 kap. Buffringsprogram

Syftet med signeringsmodulen är att säkerställa att buffringsmodulens data inte manipuleras. I normalläget lagras kvittodata i journalminnet, buffringsmodulens minne samt i kontrollservern. Data lagras dock kontinuerligt i buffringsmodulen och vid ett avbrott i kommunikationen med kontrollservern så finns alltså data kvar i buffringsmodulens minne. Denna information förs sedan över till kontrollservern när kontakt återupprättats. Information kommer också att finnas i journalminnet på kassaregistret.

Nivån av kontroll blir mycket hög med den föreslagna proceduren som kan vara relevant om denna nivå av säkerhet är önskvärd. Det kan därför ifrågasättas om säkerhetsnivån och komplexiteten står i proportion till nyttan. En alternativ lösning bör därför beaktas.

Hanteringen av kontrolldata samt signering utgör en mycket komplicerad procedur som förutsätter nyutveckling av tillverkare. Det kan ifrågasättas om denna komplexitet är proportionerlig i förhållande till den extra kontrollmöjlighet som är syftet med hanteringen.

Det uppstår en sårbarhet pga. mycket signalering mellan buffert och server.

Är det nödvändigt med alla olika loggar. Står detta i proportion till nyttan?

47 §

Vad är en logg för "Andra aktiviteter"? Avses en logg för framtida användning.

48 §

Varför har värdet 48 timmar för maximalt kommunikationsavbrott mellan kontrollserver och buffringsmodul valts?

7 kap. Kontrollserver

4 §

Även återförsäljare borde tillåtas anskaffa och installera EV-certifikatet. Motivering se ovan.

5 §

Även återförsäljare borde tillåtas att uppdatera listan över signeringsmoduler.

6 §

Även återförsäljare borde tillåtas att uppdatera listan över ID-strängar.

8 §

Är kontroll en gång per timme ett krav i samklang med standard för lagring på server?

10 §

Kontrollservern blir med detta krav fysiskt dedikerad. Detta är ett kostnadsdrivande krav. Virtualisering borde vara tillåtet.

12 §

Är det lämpligt att ha kontroll av kassaregister och signeringsmoduler var 10:e minut. Detta skapar en stor nätbelastning. Det är inte heller tydligt hur dessa tester ska hanteras vid avbrott.

18 §

En kontrollserver ska under minst fem år lagra data. Det är inte klargjort hur situationen med fullt minne ska hanteras.

20 §

Det definieras inte vad andra aktiviteter är. Om här inte avses en manuell logg skapad av en behörig användare så kommer detta att förbli oklart.

35 §

Även här borde återförsäljare kunna generera individuella krypteringsnycklar utifrån Skatteverkets huvudnyckel.

38 §

Är det verkligen nödvändigt med kryptering av information som förs över mellan kontrollserver och buffringsprogram.

Kryptering används för att skydda mot obehörig tillgång till information men den påverkar inte informationens innehåll. Det är svårt att se att just informationsflödet mellan kontrollservrar och buffringsenheter är av sådant intresse att det behöver krypteras.

8 kap. Sammankoppling

13 §

Buffringsprogrammet ska minst var tjugofjärde timme kontrollera att de kassaregister som är anslutna till kontrollsystemet också är sammankopplade med kontrollsystemet. Är detta nödvändigt? Vad är motivet till val av frekvens?

9 kap. Kommunikation inom kontrollsystemet

2 §

Är det givet att servertjänsteleverantörer och kassaregisterleverantörer kontinuerligt uppdaterar algoritmuppsättningar och nyckellängder enligt aktuell utgåva av NST FIPS 800-52. Om inte, blir detta krav ett avsevärt försvårande av möjligheten att i praktiken följa detta krav.

10 kap. Kontrollserverns miljö

2 §

Även här bör återförsäljare ha möjlighet att vara den som kan åläggas att uppfylla miljökraven.

4 § - 12 §

Återförsäljare bör läggas till. En tillverkare kan ha säte varsomhelst på jorden och det är då inte sannolikt att de utarbetar ledningssystem för den svenska marknaden.

Om dessa krav går utöver standardiserade krav på serverhallar skapar de extra kostnader och reducerar troligtvis antal aktörer som kommer att erbjuda serverbaserade kontrollsystem vilket i sin tur kan leda till en marknad utan konkurrens.

13 §

"Tillverkare ska regelbundet analysera insamlade uppgifter med avseende på att säkerställa att ingen obehörig åtkomst eller obehörig användning av data och system skett."

Detta krav utan närmare specifikation av innehåll i analysen och vad regelbundet avser riskerar att bli meningslös.

14 §

Är detta ett proportionerligt krav jämfört med de krav på åtkomst som ställs på andra delar av kassaregister med kontrollserver?

Kravet innebär också en extra kostnad för access, i synnerhet om tillgången behöver vara fysisk.

16 §

Manuellt förd liggare ska finnas. Är detta ett standardiserat krav i serverhallsmiljöer? Om inte kan proportionaliteten ifrågasättas under beaktande att det redan finns åtkomstloggar mm.

24 §

Avses här skapandet av individuella krypteringsnycklar? Det står inget om hanteringen av nycklar i 7 kap. 36 §.

11 kap. Kontrolldata till Skatteverket

14 §

Buffringsprogram och kontrollserver ska ge ifrån sig en tydlig visuell eller ljudmässig signal då utläsning sker. Detta blir tilläggskrav på både buffringsenhet och kontrollserver som inte nämnts tidigare.

12 kap. Tillverkning, test och dokumentation

28 §

Är det ett realistiskt och proportionerligt krav att två personer hos tillverkaren vid hantering av huvudnyckeln ska vara samtidigt närvarande.

Det framgår inte hur spårbarheten på individnivå ska genomföras.