Målnummer:	1425-04	**Avdelning:**	2
Avgörandedatum:	2004-12-21		
Rubrik:	Sekretess enligt 5 kap. 2 § 1 sekretesslagen har ansetts gälla för uppgifter om samtliga datorer med tillhörande utrustning vid en tingsrätt med avseende på tillverkningsnummer, fabrikat, typ, inventarienummer och inköpsdatum.		
Lagrum:	5 kap. 2 § 1 sekretesslagen (1980:100)		
Rättsfall:			

REFERAT

Göteborgs tingsrätt beslutade den 2 september 2003 med stöd av 5 kap. 2 § 1 sekretesslagen (1980:100) att avslå K.J:s begäran att få ut en förteckning över samtliga datorer och servrar vid tingsrätten med avseende på inventarienummer, typ, tillverkningsnummer, fabrikat och inköpsdatum. Enligt tingsrättens uppfattning var det förenat med stora säkerhetsrisker att lämna ut de begärda uppgifterna eftersom de kunde användas för en kartläggning av datorutrustning på ett sådant sätt att intrångsförsök eller virusspridning skulle underlättas.

K.J. överklagade och vidhöll sin begäran.

Kammarrätten i Göteborg (2004-02-17, Andersson, Edlund, Åberg, referent) yttrade: Enligt 5 kap. 2 § 1 sekretesslagen gäller sekretess för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd med avseende på byggnader eller andra anläggningar, lokaler eller inventarier om det kan antas att syftet med åtgärden motverkas om uppgiften röjs. - I målet har inhämtats yttranden från Domstolsverket samt Post- och telestyrelsen, PTS.

Domstolsverket anför i huvudsak följande. Med hjälp av tillverkningsnummer eller serienummer kan den som vill göra olika typer av skadliga ingrepp mycket lätt bilda sig en uppfattning av vilken typ av datorer som finns på domstolarna. Med den informationen kan man lätt ta reda på eller göra välgrundade antaganden om vilken BIOS (Basic Input Output System) de olika datorerna kör på. BIOS är en samling rutiner för in- och utmatning som utnyttjas av PC-DOS, MS-DOS och program som körs i datorer som har detta operativsystem. Eller annorlunda uttryckt; en BIOS är en sorts mycket grundläggande dataprogram som styr hårddisk, grafikkort m.m. Varje BIOS har mer eller mindre kända brister. Sådan information finns tillgänglig på Internet - om inte annat via vissa diskussionsforum. Har man information om vilken BIOS som används kan den informationen underlätta för den som vill göra ett virusangrepp eftersom den personen kan anpassa viruset efter BIOS:en. - Vidare kan de olika uppgifterna sammantaget underlätta för den som vill göra olika typer av skadliga angrepp. Uppgifter om typ av datorer och servrar, tillverkningsnummer m.m. kan utgöra grund för vidare antaganden om vilken programvara eller operativsystem som exempelvis körs på servern. En sådan kartläggning ger således grund för antaganden som kan underlätta angrepp av virus eller s.k. maskar. - Sammanfattningsvis kan således sägas att dessa uppgifter ensamma men särskilt i förening med varandra kan användas för kartläggning i syfte att stjäla datorutrustning, att göra dataintrång i Domnät (domstolarnas gemensamma nätverk) och att utsätta Domnät för virusattacker. När det gäller de två sistnämnda riskerna bedömer Domstolsverket det som särskilt riskabelt att

lämna ut uppgift om tillverkningsnummer eller serienummer. Detta gäller oavsett om de andra uppgifterna lämnas ut eller inte.

PTS anför följande. Ett datorsystem eller nätverk är uppbyggt av en mängd olika komponenter. De viktigaste och mest grundläggande av dessa är den hårdvara och mjukvara som agerar som server och olika former av brandväggar i nätverket. Precis som det när en person avser att olovligt bereda sig tillträde till en byggnad - då det är en avsevärd fördel att ha tillgång till en ritning över byggnaden - gäller motsvarande avseende datornätverk. Med tillräckligt många uppgifter avseende den hårdvara och mjukvara som nätverket fysiskt och logiskt är uppbyggt av blir möjligheterna att med framgång utföra ett angrepp betydligt större. Detta till stor del på grund av att ett angrepp i sådana fall kan bli betydligt effektivare och att eventuella övervakningssystem inte har samma möjlighet att upptäcka angreppen. - De olika uppgifter som är aktuella i målet kan utgöra delar av just en sådan ritning till ett system. Uppgifterna kommer nedan att bedömas var för sig och avslutas med en sammanfattning. - Tillverkningsnummer eller serienummer är den av uppgifterna som innebär störst säkerhetsrisk. Med ett sådant nummer är det tämligen enkelt att ta reda på mer eller mindre exakt vilka komponenter (hårdvara) en utrustning består av samt när dessa tillverkades. Med uppgifterna om hårdvara och tillverkningsdatum kan välgrundade antaganden göras om vilka operativsystem och vilken programvara som används i terminalen. Eftersom alla operativsystem och programvaror har vissa säkerhetsrisker är denna information viktig om man avser att vidta ett angrepp då informationen utgör en fingervisning om vilka verktyg och angreppsmetoder som är effektiva och verkbara. Även hårdvaran i sig kan innehålla säkerhetsbrister som kan exploateras. Uppgifterna om hårdvara är därmed inte en säkerhetsrisk endast för att informationen kan leda vidare till vilken mjukvara som används. För att göra en enkel liknelse så innebär kunskapen om typ av dörr och lås att en person med adekvat kunskap vet vilken typ av dyrk eller slägga som på kortast tid och minst märkbara sätt öppnar dörren. - Inköpsdatum samt typ och fabrikat är uppgifter som tillsammans och var för sig kan användas för liknande härledningar som tillverkningsnummer. Inköpsdatum ger en hänvisning till typ av system i vart fall på sådant sätt att det inte kan vara fråga om någon hårdvara som marknadsförts efter inköpsdatumet. Typ och fabrikat ger en mer direkt hänvisning till vilken slags hårdvara det rör sig om och därmed en fingervisning till vilka operativsystem och vilken mjukvara som troligen används. Uppgifterna får dock anses vara av sämre precision än tillverkningsnumret eftersom de inte utgör en lika exakt identifiering som tillverkningsnummer. Även om precisionen blir sämre är det dock PTS uppfattning att uppgifterna var för sig och tillsammans utgör en säkerhetsmässig risk om de sprids, låt vara inte av samma dignitet som tillverkningsnumret. - Inventarienummer får antas vara en identifikation av utrustningen från ägaren till utrustningens egen förteckning. Ett inventarienummer i sig kan knappast ha någon betydelse för någon som inte har tillgång till själva inventarielistan eller i vart fall kännedom om hur denna är uppbyggd. Tillgång till ett inventarienummer kan emellertid antas underlätta vidare eftersökningar efter information om vilken typ av utrustning som döljer sig bakom inventarienumret. Om det i inventarienumret ingår någon slags tidsangivelse ger inventarienumret också en hänvisning till inköpsdatum varför delvis samma överväganden som redovisats för denna typ av uppgift ovan kan anföras även här. Inventarienummer får dock av dessa fyra typer av uppgifter anses vara den som är av minst risk ur en säkerhetsaspekt. - Det är sammantaget PTS uppfattning att ovan nämnda uppgifter så vitt de avser datorer och terminaler som ingår i ett nätverk, särskilt om nätverket är åtkomligt utifrån, utgör uppgifter som var för sig och sammantaget kan innebära säkerhetsmässiga risker. I synnerhet tillverkningsnummer utgör en känslig uppgift men även uppgifterna i övrigt kan härledas till information som är säkerhetsmässigt känslig. Av de fyra uppgifterna får inventarienummer sägas vara av lägst säkerhetsrisk. - Även om uppgifterna i sig i vissa fall inte kan anses vara av direkt skadligt material som ensamt kan användas för att olovligt bereda sig tillgång till systemet i sin helhet utgör de uppgifter som är

ett viktigt led i efterforskningen av svagheter i systemet vilket i sin tur är en viktig del för att få kännedom om angreppsmöjligheter. Sådana svagheter ger förvisso ofta inte någon person en direkt tillgång till systemet men kan avsevärt höja effektiviteten för ett angrepp. Med effektivitet avses både snabbheten i ett angrepp och de möjligheter en angripare har att dölja sitt angrepp. Effektivitet är synnerligen viktig vid ett angrepp av detta slag, inte minst med tanke på att de möjligheter till skydd som finns ofta har svårigheter att skilja på tillåten och otillåten åtkomst. Ett framgångsrikt angrepp kan naturligtvis orsaka mycket stora skador.

Kammarrätten gör följande bedömning. - Beträffande uppgifter om tillverkningsnummer anser kammarrätten, med hänsyn till vad Domstolsverket samt PTS anfört, att ett utlämnande kan antas motverka syftet med de säkerhetsåtgärder som vidtagits för att skydda domstolens datasystem. Det föreligger därmed hinder enligt 5 kap. 2 § 1 sekretesslagen att lämna ut begärda uppgifter om tillverkningsnummer. Också kännedom om datorernas och servrarnas fabrikat, typ, inventarienummer och inköpsdatum kan, i vart fall om uppgifterna föreligger tillsammans, antas innebära en sådan risk som beskrivits ovan. Även dessa uppgifter omfattas därför av sekretess och skall således inte lämnas ut. - Kammarrätten avslår överklagandet.

K.J. fullföljde sin talan.

Regeringsrätten (2004-12-21, Lavin, Billum, Eliason, Almgren, Kindlund) yttrade: Skälen för Regeringsrättens avgörande. Regeringsrätten gör samma bedömning som kammarrätten.

Regeringsrättens avgörande. Regeringsrätten fastställer kammarrättens dom.

Föredraget 2004-11-24, föredragande Nilsson, målnummer 1425-04

Sökord: Allmän handling sekretess eller inte

Litteratur:
