Beslut om portspärr i Chalmers Internetanslutning

1 Uppdragsgivare/Förvaltare

Vilk-en/a organisation-/er vill ha en lösning

Chalmers datorincidentgrupp (IRT) och Chalmers datanätgrupp (CDG).

1.1 Vem/vilka personer/funktioner med mandat vill och kan beställa en lösning

IT-beredningen.

1.2 Vilk-en/a organisation-/er skall förvalta lösningen

Chalmers datornätgrupp (CDG).

2 Önskemål

Beskriv möjlighet-en/er / probleme-t/n ur ett uppdragsgivar/användar-perspektiv

Chalmers datorer som är anslutna till nätet utsätts ständigt för olika angrepp och avsökningar då angripare söker efter sårbarheter. I vissa fall kan man med enkla medel försvåra eller förhindra dessa angrepp och undersökningar genom att spärra viss trafik in till Chalmers nätverk.

3 Lösning

*Beskriv lösningen ur ett uppdragsgivar/användar-perspektiv **och** hur det realiseras med hjälp av "IT" (beskriv med så lite IT-termer som möjligt).*

Vi föreslår att IT-beredningen ger CDG i uppdrag att spärra vissa "portar" för trafik in till Chalmers nät. IRT fungerar som remissinstans åt IT-beredningen för att utreda konsekvenser och effekter av ändringar i listan över spärrade portar.

Förutsättningar för att denna lösning skall vara "enkel" är:

1. Portspärren omfattar hela Chalmers nätverk (129.16.0.0/16, ungefär *.chalmers.se) utan undantag.
2. IT-beredningen fattar beslut om eventuella tillägg eller strykningar från listan över spärrade portar.
3. IT-beredningen informerar om förändringar i portspärren via Chalmers interna nyheter.

4 Avgränsningar

Närliggande områden som inte ingår i lösningen

Om förutsättningarna ovan inte är uppfyllda kan IRT och CDG inte åta sig uppdraget.

5 Alternativ

Vilka alternativ är undersökta och varför är de inte rekommenderade

IRT och CDG har diskuterat andra lösningar med mer eller mindre avancerade brandväggar. Alla dessa lösningar kräver långa förarbeten och betydande investeringar. Den föreslagna lösningen kan implementeras snabbt och det går fortfarande att utforska de andra alternativen.

6 Tidsplan

Tid för utredning/planering/beslut, tid för genomförande, tid för drift, tid för avveckling

Efter beslut kan portspärren tas i drift omgående.

7 Kostnader

Livscykelkostnader (Exempel på faktorer: Implementationskostnader, utbildning av kund, intern tid, driftskostnader samt eventuella avvecklingskostnader skall uppskattas)

Portspärren "kostar" en viss prestanda i den utrustning som utför den. CDG gör dock bedömningen att tillräcklig reservkapacitet finns för att detta inte skall utgöra ett problem inom överskådlig tid.

Portspärren medför förmodligen en del kostnader för de som idag använder aktuella tjänster hemifrån eller från externa kontor. Dessa är dock av engångsnatur (t ex kostnad för installation av och utbildning för VPN).

8 Lönsamhetskalkyl

Vad "tjänar" uppdragsgivaren på "investeringen"

Att besluta om att vi kan spärra portar och hur dessa portar skall utpekas är en förutsättning för att kunna genomföra denna typ av spärr.

Lönsamheten när man spärrar en port måste bedömas från fall till fall, se appendix A.

9 Finansiering

Vem betalar (med vilka pengar)

Lösningen medför låga kostnader för CDG och IRT, endast några få timmar arbetstid. Kostnader för att ge stöd åt användare som arbetar hemifrån får respektive avdelning ta.

10 Beslut

Vilk-et/a beslut skall fattas

IT-beredningen beslutar att ge CDG uppdraget att införa spärrar för vissa portar. IT-beredningen ansvarar för förteckningen över vilka portar som skall spärras.

Datum	Roll	Beslutsfattare (namnförtydligande)	Signatur

A Portspärr av Windows-tjänster

Datorer som kör operativsystem från Microsoft (t ex Windows NT, Windows 95/98, Windows 2000 eller Windows XP) är utsatta för en ständig ström av angrepp. Oskyddade så kallade "shares" är och har under lång tid varit en av de vanligast målen för attacker. Inom Chalmers finns många datorer med dessa operativsystem som saknar tillräckligt skydd vilket leder till en mängd störningar och problem, bland annat:

- Intrång varefter maskinerna används för att sprida upphovsrättsskyddat material (t ex film, programvaror) eller vidare angrepp.
- Användare kan inte använda sina konton. Ett par sektioner har upprepade gånger haft detta problem med följd att datorbaserade laborationer inte kunna genomföras.

A.1 Vilka för/nackdelar finns med portspärren?

Genom att spärra åtkomst av Windows-tjänster inom Chalmers från resten av världen kommer problemen att minska kraftigt. Åtgärden innebär vissa inskränkningar som kommer att irritera en del användare och tvinga dem till förändrat arbetssätt, speciellt vid arbete hemifrån/utifrån:

- Användare kommer inte kunna nå fileservers mm "utifrån" (till exempel hemifrån). Detta problem löses med den VPN-tjänst som CDG håller på att starta eller genom att "tunnla" tjänsterna med ssh.
- Vissa katalogtjänster fungerar inte längre utanför Chalmers-nätet. Samma lösning som ovan.

A.2 Lönsamhetskalkyl

Mer än 95% av de 145 maskiner med intrång som IRT fick rapporterade/upptäckte under kvartal 1 2003 körde någon form av Windows. En mycket försiktig uppskattning är att hälften av dessa intrång hade kunna undvikas om föreslagen spärr hade funnits. Vi brukar uppskatta att det kostar ungefär en arbetsvecka för varje intrång i form av bortkastad arbetstid för användaren, tid för undersökning, ominstallation och hantering.

Med dessa antaganden skulle den föreslagna spärren spara 280 manveckor per år (drygt 6 heltidstjänster).

Vad gäller kostnader finns inga direkta kostnader utöver kostnader för att hitta alternativ för bland annat filaccess. Till exempel kan det innebära kostnader för lokala driftgrupper om de behöver introducera användare till VPN-tjänsten. Dessa är dock betydligt lägre än de kostnader som dagens intrång för med sig.

A.3 Beslut

IT-beredningen beslutar att spärra följande portar för trafik in till Chalmers nätverk:

Port	**Portens funktion**
137 (TCP/UDP) 138 (TCP/UDP) 139 (TCP/UDP)	Diverse katalogtjänster inom Windows, t ex för att hitta resurser (skrivare, fileservers mm), autentiseringstjänster, behörighetskontroll.
445 (TCP/UDP)	Fileserver

Datum	Roll	Beslutsfattare (namnförtydligande)	Signatur