Version: 1.0	Version: 1.0 Ansvarig: Christoffer Strömblad (https://cstromblad.com/)							
Funktionsområde	**Org ID.**	**CSF ID**	**Kategori**	**Förmåga**	**Kommentar**	**Specifika åtgärder/mekanismer**	**Metric**	**ATT&CK Ref**
Skydda	Org-1	PR.AC-5	Åtkomstkontroll	Nätverkets integritet är skyddad	Denna förmåga syftar till att ge organisationen kontroll över vilka kommunikationsflöden som är tillåtna. Det avser exempelvis utgående kommunikation såväl som kommunikation i de interna nätverken. Genom att strikt kontrollera utgående kommunikation kommer exempelvis en majoritet av skadlig kod att förhindras. De flesta skadliga programvaror (malicious software) är tvådelade, en stage 1 och en stage 2. I första steget händer inte så mycket utöver att den skadliga koden försöker ladda ner sin payload (stage 2) där den riktiga koden finns. Genom att förhindra stage 2 från att lyckas kommer den skadliga koden inte fungera och är således oskadliggjord.	1. Centralt styrd brandvägg på klienter, exempelvis Windows Defender Firewall. 2. Brandväggsregler på klienter som förhindrar all utgående kommunikation bortsett från vitlistade applikationer och tjänster. Ex endast tillåta processerna för webbläsare att kommunicera mot Internet eller proxylösning. Opt 3a. Loggning av misslyckade försök till utgående kommunikation i central brandvägg, eller annan lämpligt placerad nätverksutrustning. Opt 3b. Loggning på klient av misslyckade försök till utgående kommunikation.	1. Antalet misslyckade försök till utgående kommunikation av tidigare icke godkända nätverksflöden. Ex. skadlig kod som försöker hämta hem sin payload över HTTPS på port 443. Opt 2. Låt lämplig organisatorisk enhet (ex. SOC/CERT) granska programen/processerna bakom försöken till kommunikation för att verifiera vilka som var skadlig kod samt vilka av dessa som bör kunna godkännas för kommunikation.	Initial åtkomst - Kompromettering av supply chain https://attack.mitre.org/wiki/Technique/T1195 *Antag att en programvara ni använder kompromitteras med en bakdörr och att programvaran inte har vitlistats för utgående kommunikation skulle det bli omedelbart uppenbart om den helt plötsligt börjar kommunicera ut mot internet.* Initial åtkomst - Spearphishing via attachment https://attack.mitre.org/wiki/Technique/T1193 *Antaget att den bifogade filen består av en downloader (stage1) som laddar ner en payload (stage2).* Central styrning Vitlistning av utgående kommunikation gör många av angriparens tekniker obrukbara. https://attack.mitre.org/wiki/Command_and_Control
Skydda	Org-2	PR.AC-4	Åtkomstkontroll	Rättigheter och åtkomstkontroll hanteras och inkluderar principer som *least privilege* och *separation of duties*.	Denna förmåga syftar till att hantera diverse rättigheter och åtkomstkontroller i organisationen. Det handlar inte endast om användares rättigheter utan även applikationer, tjänster, servrar och klientdatorer.	1. Två webbläsare används på klientdatorer där en har rättigheter att kommunicera mot det interna nätverket, men inte externa nätverk (internet) och den andra webbläsaren har inga rättigheter att kommunicera internt men däremot externt. *Denna åtgärd gör det, bland annat, avsevärt mycket svårare för en angripare att lyckas med ett phishingförsök där användare förväntas trycka på en länk i ett mail. Vidare blir det mycket svårt för en angripare att "lura" den externa webbläsaren att enumerera interna nätverk etc.*	1. Antalet misslyckade försök av den INTERNA webbläsaren att kommunicera externt mot internet. 2. Antalet misslyckade försök av den EXTERNA webbläsaren att kommunicera mot det interna nätverket.	Initial åtkomst - Spearphishing via länk https://attack.mitre.org/wiki/Technique/T1192