UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Centro Interdipartimentale Grandi Strumenti - C.I.G.S.
www.cigs.unimore.it

Misure di sicurezza ICT applicate dal CIGS

Estratto dalla premessa di: MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI, Agenzia per l'Italia Digitale (26-4-2016)
"Occorre inoltre osservare che il CCSC è stato concepito essenzialmente nell'ottica di prevenire e contrastare gli attacchi cibernetici, ragione per la quale non viene data particolare rilevanza agli eventi di sicurezza dovuti a casualità quali guasti ed eventi naturali. Per questa ragione, ai controlli delle prime 5 classi si è deciso di aggiungere quelli della CSC8, relativa alle difese con-tro i malware, della CSC10, relativa alle copie di sicurezza, unico strumento in grado di proteggere sempre e comunque le informazioni dal rischio di perdita, e della CSC13, riferita alla protezione dei dati rilevanti contro i rischi di esfiltrazione"...
"... Il raggiungimento di elevati livelli di sicurezza, quando è molto elevata la complessità della struttura e l'eterogeneità dei servizi erogati, può essere eccessivamente oneroso se applicato in modo generalizzato. Pertanto ogni Amministrazione dovrà avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi."

Premessa:
Le attrezzature ICT del CIGS (principalmente personal computer) vengono utilizzate dal personale del Centro e dagli utenti (personale universitario, dottorandi e studenti) sia per poter utilizzare la strumentazione che per elaborare i dati. Per questo motivo, al fine di poter monitorare e gestire la sicurezza informatica nel migliore dei modi senza compromettere l'operatività della struttura, dopo un'accurata analisi dell'infrastruttura informatica del Centro e, constatata la complessità ed eterogeneità delle attrezzature ICT, si è pensato di suddividere le nostre attrezzature ICT in 6 macro aree:

Area 1: Server di dominio
Area 2: PC e dispositivi ICT utilizzati esclusivamente dal personale del centro
Area 3: PC e dispositivi ICT a disposizione degli utenti per elaborazione, consultazione
Area 4: PC collegati alla strumentazione e necessari per il funzionamento degli strumenti
Area 5: Altri dispositivi, periferiche connessi alla rete e apparati di rete
Area 6: Casi particolari (valutati caso per caso)

L'applicazione delle misure minime applicate dipenderà dalla tipologia [Area] a cui appartiene l'apparecchiature informatica, al fine da non impedire il corretto funzionamento delle stesse.

Policy e misure di sicurezza GENERALI della infrastruttura di rete del CIGS. (sottorete 155.185.19)

- Disponibilità di un inventario dettagliato (IP, mac, descrizione) e costantemente aggiornato (GLPI o manuale) di tutte le apparecchiature del CIGS connesse/collegabili alla rete
- L'infrastruttura informatica del CIGS opera nella sola sottorete 155.185.19 ed è collegata alla rete di Ateneo attraverso un firewall (fortigate 90D, IP 19.254), che definisce regole di accesso e uscita di ogni apparecchiatura del Centro collegata via ethernet
- **L'accesso di qualunque apparecchiatura (in entrata e in uscita) al di fuori della sottorete del CIGS (.19) è DISABILITATO di DEFAULT (Vedi policy Fortigate)**
- L'inserimento/eliminazione degli apparecchi abilitati ad attraversare il Firewall viene gestito manualmente e tracciato
- Tutte le workstation del CIGS collegate alla sottorete 19 sono inserite nel Dominio CIGS.
  Utenti Gruppo Staff: (gestione password Aging e password history)
  Utente Gruppo Strumentazione: Limitazione di acceso da una specifica workstation di dominio: (nessuna gestione password Aging e password history)
  (Nessun privilegio di amministrazione di dominio)
- NB: esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili disattivata tramite policy di dominio
- Le apparecchiature ICT dell'**Area 4** (Identificate e dedicate al controllo strumentazione) sono bloccate dal firewall in ingresso ed uscita alla sola sottorete 19. Per tale motivo, pur rispondendo ai requisiti **[ABSC1] [ABSC2]** NON rispondono necessariamente agli altri requisiti MMS.
  Autorizzazioni temporanee (di brevissima durata e comunque tracciate) ad uscire dalla sottorete al fine di manutenzione vengono valutate caso per caso
- La responsabilitá della workstation in Area4 è a carico del direttore della struttura

MODALITA'DI IMPLEMENTAZIONE DEI REQUISITI MINIMI

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Aree di applicazione: TUTTE le aree

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Wiki + GLPI/Fusion Inventory Interni *glpi.cigs.unimore.it:8086 e wiki.cigs.unimo.it:8081*
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Wiki + DHCP Interni *wiki.cigs.unimore.it:8081 e dhcp.cigs.unimore.it*
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Wiki + DHCP Interni + IPAM di Ateneo *wiki.cigs.unimore.it:8081, dhcp.cigs.unimore.it e phpipam.unimore.it*

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Aree di applicazione: TUTTE le aree

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	GLPI+Fusion Inventory Interno, con verifiche periodiche e alert *glpi.cigs.unimore.it:8086, Archivio interno e elenco pubblicato sul nostro sito web www.cigs.unimore.it*
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	GLPI+Fusion Inventory Interno, con verifiche periodiche e alert *glpi.cigs.unimore.it:8086*

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

Aree di applicazione: [AREA 1]- [AREA 2] - [AREA 3] NON SI APPLICA ALL'[AREA 4] e [AREA 5] - [AREA 6]

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	[Area 1] (Sistemi operativi server) [Area 2] (Sistemi operativi aggiornati W10) [Area 3] (immagine SO preconfigurata che si ripristina ad ogni logon) [Area 4] Come da configurazione iniziale [Area 5] come da fabbrica [Area 6] valutato caso per caso
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	[Area 3] (immagine SO preconfigurata che si ripristina ad ogni logon) - work in progress
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	[Area 3] (immagine SO preconfigurata che si ripristina ad ogni logon)
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Memorizzate su dvd ad eccezione delle macchine virtuali, ripristinate al logoff dell'utente da sessione remota secondo una master image
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	RDP e RPC via kerberos

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

Aree di applicazione: [AREA 1]- [AREA 2] - [AREA 3] - NON SI APPLICA ALL'[AREA 4] e [AREA 5] - [AREA 6]

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	In attesa di proposte del SIRS (end point protection?)
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	GLPI+Fusion Inventory Interno, con verifiche periodiche (FUNZIONA?) e alert *glpi.cigs.unimore.it:8086*
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Attivato di default per tutte le macchine
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	In attesa di disposizioni dal SIA
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Azione collegata al piano di gestione dei rischi
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Azione collegata al piano di gestione dei rischi
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Azione collegata al piano di gestione dei rischi

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Aree di applicazione: [AREA 1]- [AREA 2]- [AREA 3] NON SI APPLICA ALL'[AREA 4] - [AREA 5]- [AREA 6]

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Gi utenti che non appartengono allo staff e gli account generici non hanno privilegi amministrativi. Le eccezioni implicano la nomina di amministratore di sistema, firma del modulo di assunzione di responsabilità e l'adesione alle MMS *Gestione delle identità utente e di dominio a cura del Si-A, gruppo gestione identità*
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Accesso domain admin loggato, minimizzato l'utilizzo con creazione superuser con privilegi limitati
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	prassi
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Staff ok (pw shibboleth), da fare per altri
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Configurato con group policy di dominio (9 mesi)
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Configurato con group policy di dominio (24 cambi)
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	File crittografato
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Chiavi conservate in file cifrato

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

Aree di applicazione: [AREA 2]- [AREA 3] NON SI APPLICA ALL' [AREA 1] [AREA 4] [AREA 5]- [AREA 6]

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Ove possibile
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	firewall e IPS filter hardware dedicato
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	i dispositvi non riconosciuti dal firewall non possono collegarsi alla rete via ethernet
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Bloccato via group policy di dominio
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Solo per utenti generici e non per lo staff
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Gestione della posta elettronica e dell'antispam a cura del Si-RS, gruppo posta elettronica
8	9	2	M	Filtrare il contenuto del traffico web.	Gestione del filtraggio del traffico web a cura del Si-RS, gruppo rete
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

Aree di applicazione: [AREA 1]- [AREA 2]- [AREA 3] NON SI APPLICA ALL'[AREA 4]-[AREA5] - [AREA 6]

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Veeam backup
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Copie di backup cifrate (Veeam backup)
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

Aree di applicazione: [AREA 1]- [AREA 2]- [AREA 3] NON SI APPLICA ALL'[AREA 4]-[AREA5] - [AREA 6]

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Password e dati amministrativi sono registrati in files crittografati
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Gestione del filtraggio del traffico web a cura del Si-RS, gruppo rete

Aree e policy applicate

L'elenco delle attrezzature IT divise per area e costanemente aggiornato é consultabile presso il CIGS

Le policy [ABSC1] [ABSC2] e [ABSC3] sono applicate su tutte le apparecchiature del CIGS

Attrezzature di Area 1 (Server di dominio e apparati di rete)

[ABSC4] : Valutazione continua della vulnerabilitá - **[ABSC5]** : Uso appropriato dei privilegi di amministratore
[ABSC10] : Copie di sicurezza - **[ABSC13]** : Protezione dei dati

Attrezzature di Area 2 (PC e dispositivi ICT utilizzati esclusivamente dal personale del centro)

[ABSC4] : Valutazione continua della vulnerabilitá - **[ABSC5]** : Uso appropriato dei privilegi di amministratore - **[ABSC8]** : Difese contro i malware
[ABSC10] : Copie di sicurezza - **[ABSC13]** : Protezione dei dati

Misure di sicurezza ICT Area 3 (Macchine virtuali a disposizione degli utenti)

[ABSC4] : Valutazione continua della vulnerabilitá - **[ABSC5]** : Uso appropriato dei privilegi di amministratore - **[ABSC8]** : Difese contro i malware -
[ABSC10] : Copie di sicurezza - **[ABSC13]** : Protezione dei dati

Misure di sicurezza ICT Area 4 (PC collegati alla strumentazione e necessari per il funzionamento degli strumenti)

Apparecchiature Collegate alla solo sottorete .19 e senza alcun accesso ad altre sottoreti e ad internet –

NON si applicano di prassi : [ABSC3]- [ABSC4]- [ABSC5]- [ABSC8]- [ABSC10]

Per quanto possibile sono disattivati eventuali ingressi frontali di porte USB

Apparecchiature in Area 5 (Altri dispositivi connessi alla rete)

[ABSC5] : Uso appropriato dei privilegi di amministratore

Apparecchiature in Area 6 (casi particolari)

[ABSC4] : Valutazione continua della vulnerabilitá : **[ABSC5]** : Uso appropriato dei privilegi di amministratore : **[ABSC8]** : Difese contro i malware :
[ABSC10] : Copie di sicurezza : **[ABSC13]** : Protezione dei dati