Indice:

1 - Concetti di base della sicurezza:
Riservatezza: ogni dato deve poter essere acceduto solo da chi ne ha il diritto
Disponibilita': ogni dato deve essere sempre fruibile e disponibile a coloro che hanno il diritto di utilizzarlo
Integrita': ogni dato deve essere "originale" e non deve poter essere manipolato e modificato da non autorizzati

Tutto qui, piuttosto semplice

2 - Minacce
In realta' la situazione è molto grave perche' intorno al BADware girano

molti molti soldi. E' una forma di business in forte crescita e una grossa possibilita' di guadagno e di finanziamento per molti, anche per scopi non leciti e/o riconducibili a criminalita' organizzata.

Ora come ora l'attivita primaria non è piu di istruzione, cultura, divertimento, ma finalizata al lucro e al guadagno. per questo c'è molto accanimento per accaparrarsi fette sempre maggiori e a volte nuove, di mercato.

Inoltre viste le potenzialita' degli strumenti (internet, infinite vulnerabilita, infinita banda e potenza di calcolo), il BADware è spesso e volentieri utilizzato per spionaggio industriale e addirittura come strumento per una potenziale guerra fredda cibernetica.

3 - Scopi/Obbiettivi
Vediamo questo cosa implica e cosa ci troviamo in realta' ad affrontare nella vita vera di tutti i giorni: malviventi che sfruttano qualsiasi cosa per:

a) fare SPAM con lo scopo di vendere merci (spesso illegali: droghe, armi,
sostanze proibite)
b) Phishing: prelevamenti su conto corrente/carta di credito/paypal
c) Profiling: vendita di dati personali per profilare un potenziale utente a cui mandare SPAM miratissimo: ad una azienda conviene di piu' mandare pubblicita' mirata verso pochi potenziali acquirenti interessati (che poi comprano) piuttosto che mandare pubblicita' a tutti che magari non compreranno mai
d) Social Phishing: raccolta di credenziali di account social per aggiungere «mi piace» a campagne finanziate, per aumentare per esempio la reputazione di un gruppo di persone o di una azienda, oppure per effettuare recensioni di aziende/venditori_su_ebay/negozi_on_line, oppure impersonare un'altra persona e fare tutto a nome suo
e) Data Mining: raccolta e vendita di tutti dati potenzialmente utili: contatti, numeri di telefono, email valide e funzionanti, account di posta, documenti
f) DoS e DDoS: interrompere un servizio (concorrenza, attacco cibernetico)
g) Estorsione: antivirus finti (che appena si sono installati ti obbligano
a pagare per "riavere il PC") e virus bloccanti (ransomware)

Poi c'e' del BADware che fa cascare le braccia sapendo da chi e' usato:

Sappiamo che il governo americano ha obbligato gli sviluppatori dell'algoritmo RSA a inserire due backdoor, in modo che il governo sia comunque capace di decifrare gli oggetti criptati con chiavi RSA (algoritmo di generazione di numeri pseudo-casuali Dual Elliptic Curve Deterministic Random Bit Generation e l'altra sulla funzione Extended Random). Hanno hardware sconosciuto e non pubblicato. Era gia' successo negli anni 70 per l'algoritmo DES di IBM: NSA scopri' la crittanalisi differenziale (tenuta segreta) e forzo' silenziosamente l'algoritmo. Ci vollero altri 10 anni alla ricerca accademica per scoprire "da sola" la crittanalisi differenziale e mettere una patch a DSA. Intanto chissa' che trovo' la NSA in 10 anni di indisturbato lavoro.

NSA installa tramite siti web contraffati diversi software/malware per "monitorare" PC da remoto, uno fra i tanti e' stato fornito da l'italiana hackingTeam.it ed e' piuttosto potente, addirittura adesso e' uscita anche la versione per Android. Cosa deve fare in questi casi una azienda

che produce antivirus? In alcuni casi gli antivirus sono sotto processo negli USA perche' marcano come vorus e rimuovonoquesti malware di NSA. Sono stati accusato di "Favoreggiamento al terrorismo". Attualmente le case produttrici di antivirus si dividono in "quelle che rilevano e rimuovono il malware della NSA" e "quelle che lo ignorano"

Il governo tedesco ha recentemente diffuso uno "strumento di gestione remota" sui pc di persone sospette di reati. (fonte ccc). Il malware si chiama r2d2. Il problema di fondo e' che per installare il software sui PC di potenziai sospetti e' stato diffuso ovunque, utilizzando mezzi discutibili (siti web bucati, botnet) in modo che e' stato involontariamente
"installato" anche un sacco di persone che non erano indagate.
Inoltre per problemi strutturali il malware e' stato progettato talmente male che ha cosi' tanti buchi d sicurezza che chiunque può prendere il controllo completo del pc sul quale è installato: basta mettere qualche bot a scannare internet in cerca di quel programma installato e, quando trovato, installare l'exploit remoto...

Microsoft ha fatto "spegnere" dalle autorita' un servizio di DNS pubblico (no-ip.com) per "lotta alla distruzione delle botnet" causando disservizi e danni a moltissime aziende che non possono permettersi di comprare un IP statico. Sarebbe bastato tirar giu' i DNS incriminati, tramite la cancellazione dei relativi record IN A; probabilmente il fatto di aver tolto un servizio anonimo a tutti (buoni e cattivi) e' una manovra "commerciale" per fare la voce grossa e mandare un messaggio piuttosto chiaro a tutti

E' risaputo e mai smentito che c'e' una collaborazione fra i maggiori detentori di dati personali del mondo (Google, Facebook, Apple, youtube, Amazon, HotMail etc etc) e NSA, si pensa che tutti forniscano certi dati a NSA ma non sappiamo di che tipo e in che quantita'.
Google e' anche il "censore" di moltissime informazioni in nazioni di ispirazione totalitaria che pagano per selezionare prima i risultati delle ricerche (in Cina per esempio, ma chissa'...)

ToR
la rete tor, tramite protocollo p2p, garantisce un ottimo livello di privacy, sia per il cittadino comune e innocente che non vuol far sapere ai governi e agli isp cosa fa, sia per i malviventi per poter operare in pieno anonimato all'interno della rete. Ovviamente a qualcuno potrebbe dare fastidio e si registrano un sacco di tentativi volti buttar giu la rete tor: attacchi DDoS, intrusioni su macchine, server e HUB tor, addirittuta agenti della CIA hanno provato a infiltrarsi come membri nel consiglio di amministrazione della associazione "proprietaria" di ToR, in Russia hanno messo una taglia, piuttosto ridicola fra l'altro, (11.000$) a chi "neutralizza" la rete tor.

5 - Ambiente ed Ecosistema
Tramite la rete TOR oltre a garantire l'anonimato di una persona, si e' riusciti a costruire una rete enorme, completamente anonima e quasi del tutto staccata da internet. E' conosciuta come "deep web" e ci si accede tramite dei dns speciali che risolvono tld .onion e dei server che fanno da ponte.
Dentro si trova ovviamente il peggio del peggio: pedopornografia, vendita di armi, droga, sistemi di mail e messaggistica indecifrabili, compra-vendita del malware e delle vulnerabilita', soprattutto 0-day. Gli 0-day sono vulnerabilita' non documentate ne' segnalate alla casa madre con il relativo exploit. Chiaramente se viene scoperta una vulnerabilita ma nessuno la comunica al programmatore, nessuno ci

mettera mai una pezza per correggere l'errore del software, e quella breccia rimarra aperta fino a quando qualcun altro non la trovera' per conto suo. Vista la scarsa qualita' del software che viene venduto è ragionevole pensare che il grosso delle compromissioni sia dovuto proprio agli 0-day, anche se esistono macchine in rete ancora infettate dal SASSER (1999).
Giusto per capire quanto si va a spendere nel deep-web: un contratto annuale che prevede come minimo una fornitura di 25 0-day (buoni, cioe' che dureranno molto prima di essere scoperti da altri) costa circa 25.000 dollari.
Ci sono anche aziende che operano legalmente alla luce del sole che sono nate come antivirus ma hanno trovato un business migliore ricercando vulnerabilita' nei software e vendendo gli 0-day alle case produttrici (VUPEN e zdnet vendono a Microsoft).
Qualche esperto di sicurezza ha proposto alla comunita' di investire i soldi del budget per la sicurezza (spesi solitamente in acquisto di apparati, di software e di expertise votato alla sicurezza) in acquisto di 0-day sul deep-web, in modo da rendere pubbliche un numero sempre maggiore di vulnerabilita', con la speranza che sia piu' rapida la distribuzione delle patch relative... Una proposta provocatoria, almeno in parte, ma giusto per far capire quanto gli esperti del settore si sentano frustrati e fruttati (alla frutta)

Dopo aver comprato qualche kilo di 0-day, senza uscire dal centro commerciale "deep-web" ci si puo' anche comprare una piccola botnet che servira' per scansionare internet in cerca di macchine vulnerabili alle armi che abbiamo comprato. In questo modo cerchiamo i PC infetti, ci entriamo dentro, e installiamo o preleviamo quello che vogliamo.

Un altro modo per indurre le persone ad "installarsi" il malware e' comprare, sempre sul deep-web, CD-ROM pieni zeppi di dati personali: indirizzi mail validi, per poter mandare oviamente lo SPAM, ma anche link a siti di malware, numeri di telefono, numeri di carte di credito... insomma chi ha trovato dati personali li va a vendere sul deep-web e c'e' tutto un tariffario preciso... per esempio sui numeri di carte di credito il costo dipende da quanto sono "nuove" e a quale istituto bancario si appoggiano, e dal paese di appartenenza della carta (un russo o un cinese hanno un potere di acquisto molto maggiore, e presumibilmente una carta ORO e un conto in banca cospicuo, quindi costano di piu')

Un mercato del genere non potrebbe sostenersi senza degli istituti di credito appositamente preposti ai pagamenti, incassi, transazioni, cashing (trasformazioni di transazioni virtuali in moneta VERA sonante) totalmente anonimi: BitCoin & Co.
Si tratta di una moneta virtuale, che "scorre" su p2p: non esiste un server centrale che fa da istituto di credito, ma "pezzi" di banca sono sparpagliati in giro per il mondo. Gli account sono pressoche' anonimi, la trasformazione in denaro reale facile e "discreta"

6 - Statistiche:
- Le case di antivirus calcolano in 300.000 nuovi malware a settimana
- Mediamente il 60% delle mail che arrivano ad un MTA sono SPAM
- Con la BotNet ZeroAccess si riesce a guadagnare circa 18.000E/giorno
- 25 0-day di buona qualita' costano 25.000$ all'anno
- DDoS ovh ha subito un attacco DDoS spaventoso in luglio 2014 in cui venivano attaccati pesantemente i loro server. Ad una analisi del traffico
risulto' che una cospicua parte degli attaccanti erano utenti ADSL proprio di Ovh.. Erano sia vittime che carnefici... Il presidente di

Ovh in una intervista raccontava che nel giorno dell'attacco, quando hanno scoperto che gli attacchi provenivano dai propri utenti, si divertiva tantissimo... nelle settimane successive ha dovuto pagare i danni alle aziende in hosting che hanno subito disservizi, magari non era piu' cosi' allegro...

7 - Tipi di attacchi:
Abbiamo visto chi sono i personaggi che operano, abbiamo visto con quali scopi operano, come operano e in che ambiente di lavoro fanno le loro cose, adesso dobbiamo vedere come tutto questo impatta sui nostri sistemi e sul nostro lavoro.

Di seguito i principali tipi di attacchi operanti in rete... come si puo' vedere viene attaccato (e compromesso) qualsiasi oggetto che abbia un IP: attenzione a dire: io non ho SCADA nel mio istituto, quindi non mi interessa questo argomento perche' non sono vulnerabile.
Invece SI! Anche se non si hanno sistemi vulnerabili, tipo il SCADA, quindi non e' possibile essere vittime di un certo tipo di attacco, i nostri Istituti, i nostri IP, possono facilmente essere i carnefici, nel senso che noi siamo purtroppo proni ad essere veicolo di attacco a questi sistemi. Le GARR AUP richiedono che i responsabili di una rete si adoperino affinche' dalla propria rete non escano minacce per il mondo esterno. Inoltre quando vi troverete alla porta l'omino dell'FBI con in mano una denuncia perche' i vostri IP hanno buttato giu' 3 centrali atomiche in America, credo che il fatto che l'attacco non fosse intenzionale ma dovuto a un virus potra' evitarvi forse la sedia elettrica,
ma qualcosa vi fanno di sicuro!!

Quindi vediamoli tutti, chiaramente soffermandoci su quelli che ci interessano di piu', iniziero' a descrivere quelli che impattano meno sulla
sicurezza e gestione della sicurezza di un campus accademico o istituto di ricerca, man mano che ci avviciniamo a cio' che ci riguarda da vicino, man mano che possiamo intervenire per mitigare o risolvere una situazione,
oltre alla descrizione vi daro' delle linee guida o metodi per intervenire.

7.1 - Attacchi PoS
Quando si va in un negozio e si "striscia la carta" sappiamo che la nostra
carta diventa alla merce' di coloro che l'hanno scrisciata. Ovviamente e' interesse del negoziante proteggerla, ma a sua insaputa tutti i dati della carta possono essere comunicati ad un C&C server e venduti al mercato nero delle carte di credito valide.

I terminali PoS mediamente sono macchine windows e purtroppo oggi giorno sempre piu' terminali sono attaccati alla rete, per diversi motivi:
- l'hardware del PoS e' noleggiato e il noleggiatore ha bisogno di un canale per entrare sul PC e modificare o riparare il sistema da remoto. Le interfacce di gestione oltre ad aprire l'IP del PoS a tutto il mondo (esponendo quindi una macchina windows sulla rete pubblica) sono spesso deboli in sicurezza e soprattutto vengono usate le password di default oppure nessuna password per la gestione.
- la macchina a cui e' attaccato il PoS e' anche quella dove si fanno le fatture che poi devono essere inserire sul server della contabilita' oppure altrove: in questo caso per esempio il terminale puo' non avere un IP pubblico, e nemmeno raggiungere o essere raggiungibile dall'esterno, ma essendo comunque in rete nella intranet puo' essere

raggiungibile da qualsiasi macchina della rete interna che puo' essere virussata e puo' comunque inoculare il sotfware di "copia delle carte di credito" sul terminale.

In ogni caso il malware che alla fine riesce ad installarsi sul terminale e' in grado di accedere al lettore fisico di carte quindi si legge non solo il numero della carta e il CVV (che vengono venduti da 0.01$ a 5$ a carta sul deep-web), ma anche tutti i dati che stanno nella striscia (si chiamano "Track2 data" e sono molto utili ai malviventi per la clonazione hardware della carta e costano fino a 100$ a carta sul deep-web),
eventuali PIN di protezione o password, e manda tutti i dati al C&C server.

Statisticamente purtroppo questo e' un tipo di attacchi che sta crescendo molto (poiche' sempre piu' terminali vengono messi in qualche modo in rete), anche se ovviamente, vista la crescita del problema, sia le banche che i produttori di PoS che quei negozianti che sono consapevoli del problema, stanno cercando di migliorare la situazione (per esempio tramite carte con chip&pin piuttosto che a banda magnetica). Purtroppo indipendentemente dal sistema che si usa per leggere il contenuto di una carta, alla fine i dati passano dal terminale e sono quindi comunque a disposizione di un eventuale malware installato appositamente.

Impatto per noi:
Assumendo il fatto che gli istituti non abbiano un terminale PoS per ricevere pagamenti, l'impatto per noi e' di veicolare la propagazione e l'infettivita' del malware che, allargandosi sempre di piu', ha piu' possibilita' di scovare fra tutte le macchine del mondo, quella che ha il PoS intallato.

I virus/malware attualmente conosciuti che si occupano di bucare i PoS e che possono stare sulle nostre macchine sono:

backoff il piu' famoso
ChewBacca
BlackPOS
Infostealer.Reedum.B

7.2 - Sistemi SCADA
SCADA significa supervisory control and data acquisition e sono sistemi di controllo e monitoraggio di macchinari anche complessi.

esempi:
centrali elettriche
distribuzione elettrica
estrattori e raffinerie petrolifere
acquedotti/dighe
erogazione ossigeno, celle frigorifere negli ospedali
Satelliti: gestione orbita, software, radio di bordo, ripetitore radio

Una parte di SCADA si occupa di inviare alle macchine i comandi necessari a far loro svolgere il loro lavoro; l'altra parte di SCADA e' piu' recente e si occupa di monitorare il corretto funzionamento di un macchinario oppure le sue necessita' (piu' corrente, piu' materia prima da elaborare, malfunzionamento ad uno dei motori etc etc) questa parte si e' sviluppata man mano che i macchinari stessi diventavano piu' "intelligenti" e capaci di dialogare con i terminali, invece che di prendere
ordini soltanto.

SCADA inizialmente era un sistema 1:1 macchinario:terminale. Ogni macchina aveva il suo terminale di controllo da cui fare le operazioni.
La seconda generazione di sistemi SCADA ha architettura distribuita 1:N: un terminale di controllo per molti macchinari. Il collegamento e' veicolato tramite protocolli proprietari, non ancora standardizzati e sconosciuti.
Il terminale non e' connesso in nessun modo a nessun'altra rete
Terza generazione: Networked
si passa ad una gestione N:N: molti terminali (distribuiti negli uffici del personale preposto al monitoraggio) controllano uno o piu' macchinari.
Per rismarmiare denaro solitamente si usa lo stesso PC che il dipendente usa per lavorare, leggere la posta etc etc... cioe' un computer connesso a internet.

Eccoci qua.
Alcuni ricercatori sfidarono il mondo dicendo di esser capaci di trovare 100 bug in 100 giorni su SCADA. Alla fine dei 100 giorni avevano trovato piu' di 1000 bug.

Cosa si trova davanti un tizio che ha appena bucato il PC di un dipendente di una centrale nucleare:
- un sistema di controllo considerato (falsamente) sicuro di default (attraverso la "security through obscurity" cioe' sistemi sconosciuti ai piu' di cui si trova scarsa informazione disponibile, facilmente reperibile e gratuita, spesso coperta da copyright per brevetti, il fatto che i macchinari siano in sicurezza fisica, il fatto che il macchinario sta sulla intranet)
- un sistema molto vecchio (comprare un nuovo reattore nucleare solo perche'
parla in maniera diversa e piu' sicura con il proprio terinale non conviene)
- un software di controllo "abituato" e tarato alla prima generazione, quando era attaccato al macchianrio via "seriale" => nessun controllo accessi, password, utenze diversificate etc etc
- un sistema che non implementa crittazione a nessun livello (dati o comunicazione)

Oppure se il reattore e' piu' nuovo
- VPN per accedere al terminale (ma se buco il PC dell'operatore automaticamente sono in VPN con lo SCADA)
- crittazione delle comunicazioni
- sistemi embedded intelligenti con "autocontrollo" accessi e permessi spesso linux embedded vecchissimi e bucatissimi

Impatto per noi:
assumo che nessuno abbia da comandare aggeggi SCADA, altrimenti la cosa migliore da fare e' staccare totalmente i sistemi di controllo dalla rete o da PC che sono connessi alla rete. Oppure comprarsi dei macchinari nuovissimi e sicurissimi (e costosissimi)

Per quanto ci riguarda possiamo essere veicoli attraverso i seguenti virus:

Stuxnet: era nato come worm che il governo americano voleva spedire in Iran per controllare se avessero le centrali nucleari ed eventualmente farci qualcosa. Alla fine tramite Stuxnet, che ha un sofisticatissimo software che parla PLC (il linguaggio di programmazione dei macchinari), sono riusciti a distruggere 1/5 delle centrifughe nucleari, che si occupavano di arricchire l'uranio, in tutto l'Iran. L'unico problema e'

che si e' diffuso in tutto il mondo e attacca apparati Siemens: sono vulnerabili un sacco di altre organizzazioni.

Flame: fa la stessa cosa di Stuxnet: attacchi a pezzi di eventuali prototipi di centrali nucleari in Iran.
Entrambi fanno parte dell'"Operation Olympic Games" iniziata da Bush e proseguita da Obama, un probetto di guerra cibernetica in grande stile.

Havex - Backdoor:W32/Havex.A. E' fantastico perche' inizialmente per installarsi e' stato bucato il sito delle case madri e inserita la backdoor
direttamente nell'eseguibile di installazione del software di controllo dei macchinari che gli utilizzatori scaricavano fiduziosamente dalla casa madre di produzione del macchinario.
Una volta installato "per forza" sul PC di controllo puo' fare tutto.

Tutti questi voris fanno pesanti scanning della rete allo scopo di trovare
sistemi SCADA, quindi intasano e quando trovano qualcosa tentano di entrare

7.3 - Domotica:
E' la quarta generazione di sistemi SCADA e sta iniziando a permeare la vita di tutti noi. Si chiama anche "Internet of Things": IoT.
Sebbene attacchi alle reti domestiche non sono preoccupanti dal punto di vista della salute pubblica, sono importanti per la propria salute, anche fisica... e di privacy ovviamente.
E in alcuni casi impattano anche sulla sicurezza generale di un istituto.
Qualche studioso sta addirittura paventando la nascita di una nuova figura
di topo di appartamento skillato che utilizzera' questi sistemi per introdursi illecitamente negli appartamenti altrui e fare il proprio comodo.

Esempi
- elettrodomestici
- controllo telecamere di sorveglianza/baby monitor
- termostati riscaldamento/condizionamento
- allarmi intrusioni
- illuminazione
- blocco/sblocco porte
- routerini/switchini da battaglia per mini reti locali
- Smart TV

il business del prossimo futuro
- controllo stato/livelli/frenata automobili
- Sistemi M2M (machine2machine)

il problema di questi oggetti, che spesso stanno in rete (pubblica!) e non sono sufficientemente protetti, e' che mancano del tutto di autenticazione
di solito si accede da rete locale (computer bacati, WiFi bucata etc etc)
hanno back-door (si chiama "interfaccia di servizio") per essere acceduta dall'assistenza remota (!)
al solito hanno embedded sistemi linux vecchissimi e bucatissimi (anche eventualmente OpenSSL super vecchio/rotto)
questi oggetti sono anche configurati cosi' male di default che spesso sono veicolo dei piu' grossi DDoS che si sono visti sulla rete ultimamente
(parlero' dopo di DoS e DDoS, anche di come mitigarle il problema nella

sezione di rete)

Gli istituti inoltre possono essere vettori di virus che scannano tutta la rete alla ricerca di questi device nel mondo.
Cosa ancora piu' importante: questi device essendo bucabili, possono essere a loro volta vettori di virus

Anche in questo caso la soluzione del problema e' tenere questi sistemi staccati dalla rete: l'operatore che ci lavora deve stare li' "in console"
senza accedere da remoto.
Se questo non e' possibile bisogna cercare di staccarla il piu' possibile dalla propria rete locale: NAT, VPN, switch dedicato solo a quel tipo di traffico fatto scorrere su una VLAN dedicata e non mashata; inserire sistemi di autenticazione aggiuntivi, bloccare tutto il traffico proveniente o diretto verso quella rete, a meno che non sia il lecito traffico dovuto a chi ci deve lavorare sopra (uno o due IP soltanto, e sperare che quei due IP non prendano mai un virus in vita loro!)

Esempi
Win32/Sality (inventato 11 anni fa) faceva tutt'altro; adesso si installa sui PC e scanna e buca device IoT)
Linux.Darlloz (virus che si installa su ARM, MIPS, insomma su device IoT e fa bitcoin miner)

Statistichina
Fra il 23 dicembre 2013 e 6 gennaio 2014 (14 giorni) c'e' stata una enorme campagna di SPAM, a mandare mail indesiderate piu' del 25% degli apparati erano router, smart-TV, e FRIGORIFERI!

7.4 - RFID:
RFID significa Radio Frequency Identification e sono tutti quei sistemi che lasciano accedere a qualcosa appena arrivi in prossimita'. Sono i classici badge, quelli radio, non a banda magnetica. Ma ci sono molti altri tipi di RFID

Esempi:
- telepass
- tracciabilita' animali domestici e da pascolo (il chip impiantato)
- Immobilizer per auto
- apertura porte
- documenti di identita' elettronici, gli skypass
- logistica e magazzino aziendale
- antitaccheggio
- tracciamento pratiche burocratiche
- tessera sanitaria con tutta la cartella clinica dentro
- telecomando apertura automobili senza premere il bottone sulla chiave

Sembra una tecnologia futuristica, con grandi possibilita' future, ma al momento e' gia' largamente utilizzata in qualsiasi campo: se attualmente eliminassero RFID non potremmo far funzionare piu' nulla.
Attualmente funzionano con un lettore fisso, un "badge" e un software di interpretazione dei segnali radio. Ogni utilizzo di cui sopra ha la propria frequenza radio, stabilita da diversi standard ISO.
Per completezza nel futuro e' appena uscito un nuovo ISO (ISO 18092 NFCIP-1 e ISO 21841 NFCIP-2) che rovescia completamente la struttura "lettore - badge - software": il lettore diventa lettore/scrittore e puo' comunicare in lettura/scrittura non solo con il badge, ma anche con un altro lettore/scrittore, realizzando una rete mesh di RFID.
Sara' usato facilmente sui cellulari trasformando i cellulari in

dispositivi lettori/scrittori soprattutto per effettuare pagamenti, biglietti, titoli di viaggio, moneta elettronica.

E' facile bucarli: basta prendere un Arduino e attaccargli un ricevitore radio sulla frequenza che ci interessa. Quando passa una persona con in tasca il badge da copiare, Arduino la sente e registra cosa c'e' nel badge.
A questo punto basta comprarsi un badge vuoto e metterci dentro quello che e' stato letto. Fatto e sperimentato al BlackHat USA 2014.

E' facile sentirsi sicuri: questo luogo e' sicuro perche' ci vuole il badge per entrare! Proprio questa sensazione di sicurezza fa si' che il sistema non preveda nessun ostacolo aggiuntivo tipo un sistema di utente/password oppure una crittazione del dato che sta sul badge.
Un'altra strada per rendere piu' sicuri questi oggetti e' quella di spostare la frequenza radio da 125KHz (che si leggono anche a grande distanza) a frequenza UHF che si possono leggere al massimo a 10cm
Ma ancora non c'e' quasi niente di tutto cio'.

Quindi le problematiche sono svariate sia di sicurezza che di privacy:
- tracciamento di persone
- clonazione
- furto di identita' (e di automobile)
- Carta di credito Contactless... ci possiamo fidare?

Impatto per noi: tutti abbiamo le nostre sale macchine protette da badge, che ci possiamo fare?
Una cosa che sembra sciocca: comprare i borsellini che non fanno passare i 125KHz, ce ne sono a migliaia su internet che li vendono
https://www.facebook.com/IdentityStronghold non li conosco e non voglio far pubblicita, e' solo un esempio
Cosi' nessuno puo' leggerli. L'inconveniente e' che per entrare devi tirarli fuori dal borsellino e non vale tenerli in tasca

7.5 - Attacchi Cloud
Un esempio di utilizzo diciamo "improprio" del Cloud:
- estrema facilita' di farsi migliaia di account anonimi con spazio disco e banda pressoche' illimitati sui maggiori fornitori di servizi cloud (amazon, google etc etc)
- estrema facilita' di installare migliaia di BOT sui suddetti account
- Risultato:
  * circa 1750$ a settimana guadagnati tramite litecoin
    (impropriamente, ma LEGALMENTE!)
  * password cracking sfruttando la pressoche' infinita potenza di calcolo
  * click fraud
  * DDoS (banda infinita)
- Featured:
  * impossibilita' di mettere filtri con da/verso Amazon o google
  * legalmente non e' frode (solo rottura di qualche "Term of Service")

Altro esempio: le foto private dei VIP
Un altro attacco cloud e' stato quello perpretrato verso il cloud Apple, il risultato e' stata la pubblicazione di tutte le foto salvate dal telefonino al cloud di qualche decina di VIP.
Le foto sono state postate per la prima volta su 4Chan/b (dove e' nato Anonymous) da un tipo che vanta di aver preso anche molto altro.
Nessuno ancora ha comunicato come ha fatto, presumibilmente e' stato uno di questi fattori:
 - qualcuno ha indovinato l'email e la password

- qualcuno ha indovinato la mail e la domanda segreta e si e' fatto spedire la password o se l'e' fatta resettare
- qualcuno ha SPAM-mato l'attrice inducendola in qualche maniera a fornire lei stessa utente e password

Attualmente non risultano buchi di sicurezza nel software e l'utilizzo di 0-day e' abbastanza improbabile in questo caso (cosi' dice Apple).

Che lezione impariamo da questi fatti e cosa ci interessa per la nostra realta' di istituto?

1- L'istituto offre servizi cloud: f34r!
Sono macchine normali, principalmente linux, che oltre a fare i normali servizi linux "parlano fra di se'" con protocolli differenti a seconda del software usato (quindi dal punto di vista della messa in sicurezza oltre a hardenizzare e rendere sicuro il sistema operativo e i servizi erogati introduco un'altra variabile da monitorare e hardenizzare: il software di gestione del cloud)
    * pianificare e controllare il sistema di accessi e permessi
      * escludere se possibile la possibilita' di offrire il servizio a personale esterno, oppure non autenticato
      * verificare e testare frequentemente il funzionamento, i log, eventuali stranezze
      * pianificare regolari pen-test o vulnerability assesment

2- L'istituto utilizza servizi Cloud di terze parti (esempio GARRbox)
   * Vedere che il servizio offerto sia compatibile almeno con i punti sopra descritti
   * leggere bene i termini del servizio in considerazione della privacy e sicurezza dell'utente

3- l'istituto veicola attacchi verso sistemi Cloud (i soliti virus&co)

=======

7.6 - Attacchi (e difese) classici
Adesso entriamo in un campo che ci riguarda tutti piu' da vicino.
Chiamo questi attacchi "attacchi classici"

- sistemi operativi
- servizi
- applicazioni client
- applicazioni server
- dispositivi vari (stampanti, scanner, fax, router wifi)
- mobile
- IPv6
- apparati di rete
- topologia di rete
- policy di sicurezza

Ho messo il mobile nella categoria delle minacce piu' interessanti perche' attualmente e' una delle maggiori sfide da affrontare per un istituto: prima il mondo si divideva in interni, che avevano una stanza e avevano il computer fornito dall'Istituto stesso, gia' configurato secondo le proprie policy e i propri software; gli esterni potevano utilizzare i PC comuni delle sale calcolo oppure della biblioteca. Se arrivava un esterno col proprio PC doveva andare all'ufficio rete e farsi dare un IP dal sistemista registrandosi in qualche maniera, o prendendo un IP dal DHCP che pero' non poteva fare quasi niente a parte webbare e leggere la posta.

Quindi il mondo di un sistemista o lavoratore sulla sicurezza informatica era:
- il mondo di tutto quello che e' mio e gestisco io
- tutto il resto del mondo
i confini sono ben chiari, stabilire delle policy e' abbastanza lineare, controllare periodicamente le proprie macchine piuttosto banale...

Adesso invece ognuno arriva col proprio PC personale sul quale non abbiamo nessun controllo: ne' sul software installato ne' sulla eventuale presenza di virus e/o antivirus, ognuno oltre al PC si porta dietro mediamente un tablet (io me ne porto due!) e un telefonino e tutti questi oggetti si vogliono attaccare alla wireless. Ho anche visto gente (studenti) che addirittura si portano dietro un router wireless per farsi un piccolo nat con i propri dispositivi, oppure per dare accesso wireless agli amici che non hanno account nella struttura e che aspettano fuori dall'edificio... non c'e' piu' un confine netto fra quello che e' "la rete aziendale" e quello che non ci appartiene non possiamo sapere velocemente se il traffico e' dovuto a roba "mia" o a esterni... purtroppo
non ha piu' neanche molto senso porsi una domanda del genere perche' i confini sono proprio spariti.
Ma la responsabilita' del traffico che esce dalla nostra rete rimane dell'istituto.
E noi ci dobbiamo adoperare affinche' possiamo identificare senza ombra di dubbio chi accede alla nostra rete e affinche' dalla nostra rete non escano robe non compatibili con la AUP.

Ecco un'altra cosa a cui dobbiamo pensare a fondo: dobbiamo riprogettare tutte le strategie di sicurezza guardando alla realta' attuale, la quale ci dice che l'analisi e la manipolazione del traffico in ingresso non e' piu' sufficiente a garantire un livello di sicurezza accettabile: e' sicuramente giusto e doveroso chiudere la porta 80 in ingresso e aprirla soltanto agli IP che sono espressamente dei server web accedibili dall'esterno, ma NON BASTA.
La necessita' attuale e' di filtrare anche il traffico IN USCITA perche' adesso e' da li' che viene l'80% del male: l'80% delle macchine bucate si infetta andando a vedere un sito web bacato o giocando a un giochino online: cose che non potremo mai impedire a priori con nessun filtro.
Ma quando una macchina e' virussata inizia a fare brutte cose in uscita: raccolta e spedizione di dati personali, SPAM, scanport, DoS, comunicazione con C&C server...
ed e' a questo punto che possiamo e dobbiamo intervenire: riconoscendo il traffico brutto uscente e bloccandolo.
Lo vedremo durante la prossima sessione

Minacce e Attacchi Classici
Sono ovviamente gli attacchi piu' comuni che coinvolgono proprio i sistemisti di rete e sistemi.
Grazie agli 0-day, sia per windows che per linux, qualsiasi sistema operativo e' molto meno sicuro di qualche tempo fa. Quindi vediamo cosa si puo' fare per limitare i danni

Ci occuperemo di:
Sistemi operativi/servizi
applicazioni client
applicazioni server
dispositivi vari
apparati di rete

7.7 - Sistemi operativi/servizi

Rimangono valide le vecchie politiche di sicurezza:
chiudere tutte le porte e i servizi che non servono
mettere possibilmente le macchine dietro NAT (soprattutto se client)
aggiornare anche quotidianamente il sistema operativo e le applicazioni (per windows lasciare abilitato il windows update in modo che lo faccia da solo senza l'intervento umano)

Una cosa molto importante che vale sia per windows che per linux: quando un sistema operativo va "fuori supporto" significa che nessuno rilascera' mai piu' un aggiornamento di sicurezza. Questo significa che tutti gli 0-day e le vulnerabilita' note e non patchate al momento della chiusura rimarranno brecce aperte per sempre nel sistema. Per la gioia di chi non ha neanche bisogno di comprarsi le vulnerabilita' perche' sono sempre le solite.
Quindi e' consigliabile prevedere una strategia "di uscita dai sistemi obsoleti" soprattutto in riferimento a windows XP (e precedenti) e i linux vecchi non piu' supportati.

7.7.1 - Hardening Windows
Di seguito una descrizione dettagliata di come chiudere il piu' possibile windows in modo da limitare al massimo i danni. I passi da fare sarebbero molti e piuttosto lunghi (diverse ore), e' consigliabile fare tutto e "perdere" tempo una volta soltanto, fare una macchina fatta bene, e clonarla per tutte le macchine di ateneo. Chiudere o comunque hardenizzare
una macchina significa chiuderla il piu' possibile: anche l'utente potrebbe
risultare impedito in alcune sue funzioni. Bisogna trovare un compromesso fra sicurezza e usabilita': per questo ho catalogato alcuni suggerimenti come PARANOID, in modo da far capire che con quel sistema si mette piu' in sicurezza la macchina, ma con un impatto "visibile" sull'usabilita'.

a) Partiamo da una macchina vuota, facciamo installazione, Service Pack, e Windows Update.
Una cosa che non si fa mai ma invece e' fondamentale: durante l'installazione
il PC e' super-vulnerabile, dovrebbe stare fuori dalla rete fino a quando non e' tutto installato e confgurato.
L'eventuale Service Pack non inserito nel CD di installazione dovrebbe essere scaricato a parte e installato da chiavetta/CD-ROM
Per installare off-line anche gli aggornamenti successivi al service pack si puo' utlizzare un programmino che si chiama "WSUS Offline Update": il programma scarica gli aggiornamenti windows e li salva in una chiavetta
o CD-ROM da dare in pasto al PC dopo aver installato il SP.

b) Meno privilegi per tutti
creare immedatamente uno standard user account con meno privilegi, e utilizzare l'account privilegiato solo per le installazioni di software, aggiornamenti. Cambiare le password di default degli utenti SYSTEM, admin, ADMINISTRATOR. Metterle di almeno 15 caratteri con maiuscole, minuscole, numeri, segni di interpunzione.

c - PARANOID) Controllo Account Utente (UAC) al massimo livello (chiede conferma per molte cose, ma evita di commettere errori, specialmente per Internet Explorer)
Control Panel\All Control Panel Items\User Accounts
\Change User Account Control Settings
spostare il cursore piu' in alto possibile

d) Modificare il profilo di rete
Indipendentemente dall'uso che si fara' del PC, conviene configurare il proprio profilo di rete come "Public" che fa meno pasticci sulla rete locale.
Il profilo "home" va a carcarsi da solo sulla rete altri PC, dispositivi e fa un gran traffico.
Il proflo "public" e' da "internet cafe'" e non va a cercare niente da solo
Se la macchna sara' parte di un dominio allora scegliere il profilo "work"

e) Configurazione di rete e Protocolli
- Abilitare IPv4: quello che serve veramente e' solo IPv4. Tutto il resto apre delle VORAGINI e va disabilitato.
- IPv6: Per quanto riguarda IPv6 ne parlo dopo in una sezione apposta, se non serve va disattivato
- disabilitare Disabling NetBIOS over TCP/IP
- disabilitare Discovery protocols (serve per fare il disegnino della rete)
- disabilitare File and Printer Sharing se il PC non condivide ne' file ne' stampanti "proprie"

Qundi sul pannello di rete i consigli sono questi:
Control Panel\Network and Sharing Center \ Local Area Connection\ Properties

Disabilitare:
Client for MS Networks
File and Printer Sharing
QoS
Link Layer Topology Discovery Mapper IO Driver
Link Layer Topology Discovery Responder
Internet Protocol version 6

Selezionare IPv4 \ Properties \ Advanced
Dentro il DNS tab: disabilitare "register this connections address in DNS"
Dentro WINS tab: selezionare "Disable NETBIOS over TCP/IP"

Considerare la possibilita' di disabilitare in toto NetBios (se la macchina
non deve condividere nulla ne' accede a cartelle condivise da altri)
Control Panel / Device Manager, View menu / Show Hidden Devices /Non-Plug and Play Drivers / NETBT \ Properties
dentro Driver tab: STOP e cambiare il Type da System a Disabled
reboot per rendere effettive le modifiche. Con questa configurazione si chiude parzialmente la porta 445 (per chiuderla tutta va disabilitato il servizio "Server")

f) Disabilitare IGMP: Start \ All Programs\Accessories\command prompt
eseuire cmd da administrator e scrivere:
 Netsh interface ipv4 set global mldlevel=none

g) Disabilitare UPnP (porta 1900)
eseguire regedit
cercare la chiave HKLM\Software\Microsoft\DirectplayNATHelp\DPNHUPnP
click destro sul pannello di destra
new dword:32 bit
chiamiamola UPnPMode

assegniamo il valore 2

h) Abilitare il Firewall
controllare le porte aperte con 'netstat -abn'
i servizi essenziali che non si possono chiudere sono:
RPCss (135), Wininit.exe (49152), eventlog service (49153),
Schedule service (49154), services.exe (49155), lsass.exe (49156)
Queste porte rimangono aperte sulla macchina ma vanno bloccate sul firewall perche' servono solo alla macchna standalone e nessun altro deve poter accedere.

Poi bisogna abilitare il firewall, per stare piu' sicuri possibili il consiglio e' di bloccare tutto (paranoic e' mejo)
Come si diceva prima e' fondamentale accendere la parte di blocking e logging del traffico in uscita (outbound). Il fw va configurato con la regola standard "default deny" e aperte solo le cose che si usano.
Il firewall di Windows quando si accende ha come policy di default "deny all"
in entrata e "allow all" in uscita: va cambiato.
Il firewall di windows e' fatto molto bene per filtrare questo tipo di traffico, perche' e' un firewall di livello 7: basta specificare quali applicazioni possono passare in uscita, senza preoccuparsi del numero della porta, del protocollo e degli IP che saranno utilizzati per comunicare. Ogni volta che si installa un programma che accede alla rete dobbiamo eseguire uno a uno gli eseguibili e vedere se il blocco del fw compromette il funzionamento del programma, in questo caso va creata la regola per farlo passare.

Control Panel/Administrative Tools/Windows Firewall with Advanced Security
/"Windows Firewall Properties"

Per ogni profilo (Domain, Public, Private) va settato (LOG&DROP):
change Outbound connection = Block
Specify Logging settings for Troubleshooting > Customize
Size Limit = 32767 KB
Log Dropped packets = Yes
Specify Settings that control Windows Firewall Behavior > Customize
Allow Unicast Response: No

Per abilitare un SERVIZIO INTERNO di windows all'uscita si va nelle Firewall Rules: Outbound Rules - New Rule - Custom - Service - Customize Apply to this Service
A questo punto si cerca l'applicazione che vogliamo far passare (per esempio Windows Update) - Next - Ports and Protocol (lasciarlo) - next IP addresses (lasciarlo) - Next - selezionare Allow the Connection dargli un nome "abilitazione update" per esempio

Per abilitare un PROGRAMMA esterno dopo il New Rule si seleziona Program - next - si seleziona This program Path e si pigia "browse" cercando l'eseguibile del programma (esempio Firefox.exe)

Esempio di configurazione di firewall windows:
Questo e' un possibile elenco di cose da abilitare/disabilitare in uscita da
ripetersi per tutti e tre i profili di rete (Domain, Public, Private):

Outbound/ allow service 'Windows update'
Outbound/ allow service 'Windows Time'
Outbound/ allow program '\Windows\HelpPane.exe' (Windows Help, enables

fetching online help)
Outbound/ allow program '\program files\windows defender\msacui.exe'
Outbound/ allow program <Firefox/Chrome/Opera, whichever browser you use>
Outbound/ allow program \program files\Internet explorer\iexplore.exe
Outbound/ allow program \program files x86\Internet explorer\iexplore.exe
Outbound/ allow program <your antivirus update program>
Outbound/ allow program “%ProgramFiles% (x86)\Secunia\PSI\psia.exe”
Outbound/ allow program “%ProgramFiles% (x86)\Secunia\PSI\psi.exe”
Outbound/ allow program <path to Live Messenger>
Outbound/ allow program '\windows\ehome\ehshell.exe' (Windows Media Centre)
Outbound/ allow program '\windows\ehome\mcupdate.exe' (Windows Media Centre)
Outbound/ allow program '\Program files\Windows Media Player\wmplayer.exe'
Outbound/ disable all Core Networking rules that mentions IPv6, Teredo, and ICMPv6
Outbound/ disable Core Networking IPHTTPS
Outbound/ disable Core Networking IGMP-out
Outbound. disable all Core Networking rules that mention Group policy
Outbound/ disable the 2 rules that mentions HomeGroup
Outbound/ disable all rules for Remote Assistance
Outbound/ disable all Network Discovery rules for private profile (NB-Datagram-out, NB Name out, LLMNR UDP Out, Pub-WSD-out, SSDP-out, UPnP-Host-Out, UPnP-Out, WSD-Events-Out, WSD-EventsSecure-Out and WSD-Out.)
Outbound/ allow <Adobe Flash Update service>
Outbound/ allow <Adobe Acrobat Update service>
Outbound/ allow Core Networking DHCP-out

In INGRESSO invece configuriamo come segue:
InBound/ allow Core Networking ICMPv4 in
InBound/ allow Core Networking DHCP in
InBound/ disable Core Networking IPHTTPS in
InBound/ disable Core Networking IGMP in
InBound/ disable all Core Networking rules that mentions IPv6, Teredo, and ICMPv6
InBound/ disable the 2 rules that mentions HomeGroup
InBound/ disable all Network Discovery rules for private profile (NB Datagram in, NB Name in, LLMNR UDP In, Pub-WSD-In, SSDP-In, UPnP-In, WSD-Events-In, WSD-EventsSecure-In, WSD-In)
InBound/ disable all rules for Remote Assistance

Si puo' anche installare un firewall di terze parti (Comodo firewall) ma quello di windows funziona molto bene

i) Installare EMET (Enhanced Mitigation Experience Toolkit)
E' una sandbox, cioe' quando il sistema deve eseguire qualsiasi pezzo di codice lo esegue prima in questo ambiente protetto per vedere cosa fa e se fa cose brutte lo segnala, altrimenti passa il controllo al sistema operativo (e' identico al chroot per linux)

Queste sono le configurazioni utili di EMET per ottenere un buon risultato:
DEP - always on
SEHOP - always on
ASLR - application opt-in
defaults:
            DEP : application Opt In
            SEHOP : application Opt In

ASLR: application Opt In
Pinning: Enabled

Poi vanno aggiunti i programmi che deve chrootare: soprattutto i browser che solitamente eseguono codice malevolo da pagine web e si infettano:

Cliccare Apps - Add Application e cercare:
\Windows\System32\wuauclt.exe
\Windows\servicing\trustedinstaller.exe

poi l'antivirus, tutti i browser e programmi a rischio: chat, messenger, lettori mp3/mediaplayers, acrobat reader ... praticamente TUTTO.

E' vero che gli hacker poi se ne accorgono e sviluppano delle tecniche di evasione da EMET e dai vari chroot (emet4 e' stato dismesso proprio per questo, adesso c'e' emet5), ma prima che se ne accorgano passa del tempo e comunque molti attacchi non sono aware delle sandbox e con emet installato fallirebbero miseramente.

j) Attivare Software Restriction Policy cosicche' possono essere eseguiti dal sistema soltanto gli eseguibili che stanno dove dico io. Io diro' che possono essere eseguiti soltanto se stanno dentro \Programmi e \Windows cosi' per esempio mi sto difendendo da tutti quei malware che si installano e si eseguono dentro la Temporary Internet Files di Internet Explorer.

Questa feature non esiste in Windows Home Premium, per avere lo stesso risultato si puo' installare "Simple Software Restriction Policy" di IWR Consultancy (free)
Su Windows 7 Ultimate c'e' AppLocker che fa la stessa cosa

Configurazione Simple Software Restriction Policy 1.2 by IWR Consultancy

AdminMenuPasswordLevel=2

Aggiungere le righe seguenti sotto [Disallowed]
c:\windows\debug\WIA=1
c:\windows\Registration\CRMLog=1
c:\windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}=1
c:\windows\System32\com\dmp=1
c:\windows\System32\FxsTmp=1
c:\windows\System32\spool\PRINTERS=1
c:\windows\System32\spool\drivers\color=1
c:\windows\System32\Tasks=1
c:\windows\SysWOW64\com\dmp=1
c:\windows\SysWOW64\FxsTmp=1
c:\windows\SysWOW64\Tasks=1
c:\windows\Tasks=1
c:\windows\Temp=1
c:\windows\tracing=1

Si puo' aggiungere un ";" all'inizio delle linee seguenti per disabilitare
dei menu extra (tipo voci dal tasto destro del mouse):
;(C:\)=explorer.exe C:\
;Control Panel=control.exe
;Printers and Faxes=control printers
;Network Connections=ncpa.cpl
;Computer Management=compmgmt.msc
;Disk Management=diskmgmt.msc

```
;Registry Editor=regedit.exe
;Task Manager=taskmgr.exe
;Windows Firewall=firewall.cpl
;Command Prompt=cmd.exe
;Salamander=salamand.exe

k) Disabilitare servizi Windows non necessari:
Una guida a tutti i servizi di windows si trova qua:
 http://blackviper.com

Se vogliamo essere piu' sicuri togliamo quelli inutili
Start button/Control Panel/Administrative Tools/Services
per ogni servizio indicato nell'elenco va cliccato col tasto destro,
proprieta' e mettere type: Disable

Esempi di servizi inutili da disabilitare:
BranchCache (manual) (caches data from remote work place servers)
Computer Browser (manual) (finds other PCs in the network)
Distributed Link Tracking Client (automatic) (maintain shortcuts if
source file name has changed)
DNS client (automatic) (caches previously looked up domain names)
Function Discovery Provider Host            (manual) (HomeGroup)
Function discovery resource publication (manual) (HomeGroup)
HomeGroup Listener (manual) (HomeGroup)
HomeGroup Provider (manual) (HomeGroup)
Internet Connection Sharing (disabled) (makes PC act as router)
IP Helper (automatic) (IPv6 tunneling)
Link Layer Topology discovery mapper (manual) (network discovery)
Media Center Extender service (disabled) (turns PC into media server)
Net. TCP port Sharing service (disabled)
NetLogon (manual)
Network Access Protection Agent (manual) (reports security configuration)
Offline files (automatic)
Parental controls (manual) (empty stub for compatibility with Vista)
Peer Name Resolution Protocol (manual)
Peer Networking Grouping (manual) (HomeGroup, remote assistance)
Peer Networking Identity Mgr (manual) (HomeGroup, remote assistance)
Performance Counter DLL Host (manual) (allows remote query to performance
counters)
Performance Logs & Alerts (manual) (collects remote and local perf data)
PnP-X Ip Bus Enumerator (manual) (uses SSDP)
PNRP Machine Name Publication Service (manual) (server that responds
with a machine name)
Quality Windows Audio Video Experience (manual) (multimedia server)
Remote Access Auto Connection Mgr (manual)
Remote Access Connection Manager (manual) (dialup, VPN)
Remote Desktop Configuration (manual)
Remote Desktop Service (manual) (server allowing remote control)
Remote Desktop Service UserMode Port Redirector (manual)
Remote Registry (manual)
Routing and Remote Access (disabled)
Secondary logon (manual)
Secure Socket Tunneling Protocol service (manual) (VPN)
Server (automatic) (HomeGroup, File and Printer Sharing)
SNMP Trap (manual)
SSDP Discovery (manual)
Tablet PC Input Service (manual)
TCP/IP NetBIOS Helper (automatic)
Telephony (manual) (affects Remote Access Connection mgr/ VPN)
UPnP Device host (manual)
```

Web Client (manual)
Windows Connect Now (manual) (Wireless Setup - simplified configuration)
Windows Error Reporting Service (manual) (reports system problems to MS and fetches solutions)
Windows Event Collector (manual) (allow remote subscription to log events)
Windows Media Player Network Sharing service (manual)
Windows Remote Management (manual) (Server, listens for remote requests)
WinHTTP Web Proxy auto discovery (manual) (proxy discovery and some kind of http api)
WMI Performance Adapter (manual) (provides performance data to other PC collecting it)
Workstation (automatic) (HomeGroup)

l) INSTALLARE UN ANTIVIRUS

m) A questo punto si puo' mettere la macchina in rete, scollegarsi, entrare
con un utente Standard User e fare:
Windows Upgrade
Attivare Windows: disabilitare momentaneamente il firewall, aprire un cmd.exe come adminsitrator e lanciare
slmgr.vbs /ato

RIABILITARE IL FIREWALL

n) Installare tutti i programmi che servono (Office, Adobe Reader, Browser,
Flash plugin, driver della stampante etc etc)
Eventualmente applicare gli aggiornamenti di Office
Aggiungere regole al firewall e EMET per far passare il necessario

o) Installare "Secunia PSI"
http://secunia.com/vulnerability_scanning/personal/ (free) che si fa la lista dei programmi installati e per ogni programma va da solo a cercarsi eventuali update e le segnala. PSI avvisa anche quando il proprio sistema e' vulnerabile a 0-day noti ma ancora non patchati, cosi' che se vogliamo possiamo disabilitare momentaneamente quella vulnerabilita'.

p) Eseguire Windows Media Center perche' deve scaricarsi dei componenti

q) A questo punto:
aa) Disabilitare AutoRun: http://support.microsoft.com/kb/967715
bb) Disabilitare i Gadget: http://support.microsoft.com/kb/2719662
cc) Disabilitare i dump della memoria RAM (altrimenti accessibile agli hacker)
nella RAM ci stanno per esempio tutte le password decrittate!
Computer > Properties > Advanced System Settings > Startup and Recovery Settings - settings "Write debugging info: NONE"

dd) Disabilitare l'assistenza remota (ci sono telefonate scam che chiedono
di abilitarla addirittura):
Computer/Properties/Advanced System settings/Remote tab
deselezionare "allow remote assistance"

ff) Aumentare il numero dei Restore Points:
Right click Computer/Properties/Advanced Systems Settings
/System Protection tab - Configure - aumentare la system restore cache

gg) Abilitare la visione dei file nascosti:
Windows Explorer/ Organize/ Folder and search options / View tab
SELEZIONARE i seguenti:
Always show menus
Display the full path in the title bar
Show hidden files, folders and drives
DESELEZIONARE i seguenti:
hide empty drives in computer folder
hide extensions for known file types
hide protected operating system files

hh) Mettere la password allo screen saver
on resume logon screen

ii) disabilitare alcune feature:
Control Panel/ Program and Features
Disabilitare: Tablet PC components; Windows Gadget Platform

jj) Disabilitare AutoPlay:
Control Panel > AutoPlay
deselezionare: "Use AutoPlay for all media and devices"

kk) Accendere Windows Defender:
Control Panel/ Windows Defender - Tools - Microsoft SpyNet - Join with Advanced Membership
(se come antivirus si usa Microsoft Essentials il defender e' disabilitato
perche' e' gia compreso nell'antivirus)

ll) Abilitare la visione edgli administrative tools:
click destro su Start Button/ Properties / Start Menu - Customize
andare in fondo e su 'System Administrative Tools' settare a 'Display on All Programs Menu and Start Menu'

r) Installare Microsoft Security Compliance Manager
http://technet.microsoft.com/en-us/library/cc677002.aspx

Serve per disabilitare all'utente normale l'esecuzione degli eseguibili che stanno dentro \Windows \Windows\System32 \Windows\System
Sono programmi che non servono all'utente, principalmente a linea di comando. Gli hacker li conoscono bene e li usano per raccogliere informazioni sul sistema e su quello che possono rubare, l'utente reale della macchina invece non se ne fa di nulla. Disabilitarli all'utente e loggarsi sempre come utente garantisce che l'hacker che entrera' avra' solo i privilegi di quell'utente e non potra' eseguire i comandi a linea di comando. Bello eh

s) Internet Explorer
Protected Mode SEMPRE:
Control Panel/Internet Options/Security - selezionare Protected Mode per ogni zona. Ripetere PER OGNI ACCOUNT
ActiveX filtering:
Gear icon / Safety / - abilitare Activex Filtering. Ripetere PER OGNI ACCOUNT

IE ha una feature fastidiosa che permette agli IP della solita LAN di essere TRUSTED di default. Percio' se viene bucato un web server locale le protezioni di cui sopra non sono attive dei default e non c'e' versi

di attivarle: fare quindi molta attenzione alla propria rete locale con IE

Altri browser li fo dopo perche' vale anche per linux

t) IMPORTANTE - low Integrity
Su windows si possono mettere programmi e browser in Low Integrity: cioe' possiamo fare in modo che i file depositati da eseguire (il malware)
utilizzando il browser siano non-eseguibili. Il programma windows per far questo e' icacls.exe

Firefox low integrity
icacls "C:\Program Files (x86)\Mozilla Firefox\Firefox.exe" /setintegritylevel low
icacls "C:\Users\<yourAccName>\AppData\Local\Temp" /setintegritylevel(oi)(ci) low /t
icacls "C:\Users\<yourAccName>\AppData\Local\Mozilla" /setintegritylevel(oi)(ci) low /t
icacls "C:\Users\<yourAccName>\AppData\Roaming\Mozilla" /setintegritylevel(oi)(ci) low /t
icacls "C:\Users\<yourAccName>\Downloads" /setintegritylevel(oi)(ci) low /t

va fatto PER TUTTI GLI ACCOUNT

(PARANOID) Notare che la directory
C:\Users\<yourAccName>\AppData\Local\Temp
e' la temp generica che ho messo a low level integrity. Ma li' dentro non ci sono solo i temporanei di Firefox un hacker che arriva li' non puo' fare quasi nulla, ma sicuramente puo' guardare i temporanei anche di altre applicazioni. Per risolvere il problema bisognerebbe indicare ad ogni applicazione installata una sua temp diversa da tutte le altre e assegnargli l'integrita' low

Opera low integrity
icacls "C:\program files\opera x64\opera.exe" /setintegritylevel low
icacls "C:\Users\<yourAccName>\AppData\Local\Opera" /setintegritylevel(oi)(ci) low /t
icacls "C:\Users\<yourAccName>\AppData\Roaming\Opera" /setintegritylevel(oi)(ci) low /t

va rifatto ogni volta che si aggiorna opera perche' lui lo rimette a medium di default

u) Installare una sendbox aggiuntiva per i browser: Sandboxie
http://www.sandboxie.com/

Configurarla per il browser preferito:
click destro e poi:
delete->delete invocation> selezioare automatically delete contents of sandbox
program stop->leader programs> browser_preferito
restrictions->Internet access> only browser_preferito
restrictions->start/run access> only browser_preferito
restrictions->drop rights> selezionare 'drop rights ...'

v) Installare CHML per bloccare le directory con i documenti in lettura anche ai low integrity programs:

http://www.minasi.com/apps/ scaricare chml.exe

eseguire un cmd.exe da amministratore e lanciare:

```
cd "\user\<yourAccName>\downloads\chml"  ( or wherever you saved chml )
chml "c:\users\<yourAccName>\desktop" -ws:s:(ml;cioi;nwnrnx;;;me)
chml "c:\users\<yourAccName>\documents" -ws:s:(ml;cioi;nwnrnx;;;me)
chml "c:\users\<yourAccName>\pictures" -ws:s:(ml;cioi;nwnrnx;;;me)
chml "c:\users\<yourAccName>\videos" -ws:s:(ml;cioi;nwnrnx;;;me)
chml "c:\users\<yourAccName>\music" -ws:s:(ml;cioi;nwnrnx;;;me)
chml "c:\users\<yourAccName>\downloads" -i:l
```

Questo purtroppo non vale per gli utenti di un dominio che si prendono le home directory da remoto e usano il folder redirection

x) (quasi PARANOIC) Password:
Puo' sembrare paranoico pero' pensiamoci... ovviamente non e' necessario farlo su tutti i pc dell'istituto, ma magari qualche pc che fa anche da serverino o fa delle cose comunque importanti, o sul pc del sistemista e' meglio se queste macchine piu' importanti le aiutiamo un po' di piu'

password sul bios
disabilitare CD e USB

Inoltre valutare la possibilita' di crittare una parte del disco dati oppure tutto il sistema operativo (sconsigliato - lento - inutile) (syskey - compusec)

y) IMPORTANTE - Intrusion detection:

Tre step:
- configurazione dei log di sicurezza
- studio della normalita' e avviso quando "sgarra"
- installare oltre all'antivirus alcuni anti-spyware/malware

1) log di sicurezza
Configurare l'Event Viewer secondo la guida microsoft per utilizzarlo come IDS:
http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=21832

Allargare i log file: Control Panel/Administrative Tools /Event Viewer
allargare "windows logs" - application - 1000000
Farlo anche per Security e per System

Creare una vista apposita per la sicurezza nell'event viewer:
Create Custom View - selezionare 'By Log' - 'Event Logs'- selezionare 'Windows Logs' - spostarsi sul campo <All Event IDs> copiare incollare il numero id dell'evento - cliccare ok e salvare la view

Questi sono i numeri ID per l'event viewer che consigliamo di inserire:
4723,4724 - Change Password
4720,4726,4738,4781 - Delete, Change Accounts
4608,4609 - Startup, Shutdown
4613 - Clear Security Log
4616 - Change System Time
4617 - Unable to Log
4714,4705 - Privilege assigned or removed
4708,4714 - Change audit policy
4717,4718 - System access granted or removed
4739 - Change domain policy

16390 - Administrator account lockout
4727-4730,4731-4734,4735,4737,4784,4755-4758 - Group changes
4624,4636,4803,4801 - Account logons
4625,4626,4627,4628,4630,4635,4649,4740,4771,4772,4777 - Logon failures (KEYWORD: Audit Failure)
4672 - Admin account logons
4698 - Schedule new job
4656 - Access refused to object
3004,3005 - Windows defender finds something
4664 - Create hard link to audited file
865 - Software restriction triggered
1000 - Application Error (Event Level: CHECKMARK "Error")
1002 - Application Hang (Event Level: CHECKMARK "Error")
1037 - Protected Mode violation
7031 - Service terminated unexpectedly
4697 - Install a Service
4663 - Access audited file

alla fine SELEZIONARE: Critical, Warning and Error. Event Sources:EMET.
– EMET incidents

2) comportamento normale e anormale
E' una tecnica utile in quanto spesso e volentieri gli antivirus non sono capaci di rilevare tutti i virus del mondo, statisticamente ne vedono soltanto un 60%. Dal momento che pero' si puo' installare un solo antivirus e che ci sono virus visti solo da un particolare antivirus e non da un altro si calcola che la piu' favorevole intersezione fra gli antivirus, che massimizza il numro di virus rilevati, porta ad una rilevazione soltanto del 40% dei virus in circolazione.
Quindi puo' essere utile cercare di capire quale sia un comportamento normale (pulito) della macchina ed essere allertati quando il comportamento si discosta dalla normalita'

Per stabilire una baseline di "normalita'" si usano i seguenti programmi

A- AutoRuns: http://technet.microsoft.com/en-us/sysinternals/bb963902
fa la lista di tutte le voci del registry utilizzate dalla macchina.
Va eseguito da amministratore e gli va fatto salvare l'output su un file
Se fatto su una macchina appena installata e hardenizzata come sopra ottengo una lista pulita di tutto quello che e' ammissibile che stia sulla macchina stessa. Rifacendo l'operazione a distanza di una settimana e di un mese o comunque periodicamente, vedo le differenze nel file di ourput e posso capire se qualcuno utilizza la macchina per i propri scopi

B- ProcessExplorer: http://technet.microsoft.com/en-us/sysinternals/bb896653
E' come il TaskManager ma molto piu' utile. Lanciarlo da administrator e scrivere l'output su un file. Anche questo va periodicamente controllato

per comparare su windows si usa il comando fc: questo funziona bene per AutoRuns ma per ProcessExplorer no perche' i PID dei processi sono sempre diversi e fc vede la differenza anche se il processo e' lo stesso. In questo caso va guardato a occhio

C- netstat:
da amministratore lanciare netstat -abn > netstat-pulito.txt
ripetere nel tempo e confrontare

D- DriveQuery: e' fornito con windows ed e' a linea di comando

lanciare da amministratore un cmd.exe e scrivere:
driverquery > driverquery-pulito.txt
ripetere nel tempo e confrontare
NOTA:
al malware piace molto installarsi nei driver perche' cambiano spesso con gli update di windows e confrontando i driver rispetto alla baseline si trova difficolta' a stabilire se la differenza e' dovuta a virus o nuove features. Per risolvere il problema basta andare sul sito di Microsoft e guardarsi i driver installati da un eventuale update: se vedo un driver che non e' compreso nell'update e' sicuramente un virus

E- fingerprinting degli eseguibili
sfc e' un programma di windows che tiene in memoria i fingerprint di tutti i file eseguibili di windows. Se vengono modificati avverte e solitamente cerca anche di ripristinare quelli giusti. In questo caso la baseline e' dentro sfc, noi dobbiamo solo lanciarlo periodicamente per vedere come va:

sfc/scannow

NOTA IMPORTANTE:
i file di output della normalita' vanno salvati su dispositivi esterni USB o CD-ROM perche' gli hacker senno' possono accedere e/o modificare. Inoltre e' buona norma mettere sulla chiavetta o CD-ROM anche gli eseguibili
perche' non si sa mai che un hacker decida di modificare pure quelli: AutoRun, ProcessExplorer, netstat, DriveQuery, sfc

3- installazione anti-malware aggiuntivi
0) comparare gli antivirus: http://av-comparitives.org
http://virusbtn.com
a) oltre all'antivirus utilizzare periodicamente scannatori online: TrendMicro Housecall, BitDefender, Kapersky, Panda, ESET
b) non eseguire mai roba presa dal P2P, specialmente i crack di programmi a pagamento. mandare gli eseguibili a virustotal.com per analizzare, ricordarsi che anche se virustotal dice che non c'e' virus puo' non essere vero: il virus si accorge di stare su una sandbox e non fa quello che dovrebbe fare se fosse libero (evasion technique)
c) controllare periodicamente che l'antivirus sia vivo:
 http://www.eicar.org/86-0-Intended-use.html
 copiare le righe e lanciare sulla propria macchina
d) fare scansioni periodiche
e) valutare l'installazione di programmi aggiuntivi tipo:
   ESET anti-malware
   Webroot anti-spyware
   Gmer anti-rootkit
   Zemana AntiLogger anti-keylogger e anti-screen grabber
   KeyScrambler anti-keylogger

ZZZZ!!) Alla fine di tutto cio':
lanciare Secunia PSI
Disabilitare il flash nell'account admin:
    Internet Explorer > Gear > Manage Addons > Toolbars and Extensions
        > Show All Addons > Shockwave Flash Object - disabilitare
Abilitare IE ActiveX filtering:
    Gear icon > Safety > ActiveX Filtering
Abilitare la protezione totale:
    Gear icon > Internet options >Security tab per ogni icona
        (internet, Local Intranet, Trusted sites, Restricted sites)
abilitare: Enable Protected Mode

Questo va fatto PER TUTTI GLI UTENTI della macchina

FINITO!!!!!

Fare un bel backup, un bel punto di ripristino e una COPIA a SPECCHIO del disco, che puo' essere utile anche per clonare la macchina su altre macchine
Per la copia a specchio di puo' usare Macrium Reflect:
 http://www.macrium.com/reflectfree.aspx

IMPORTANTE:
 Quando si installa software nuovo ricordarsi di aggiornare le regole
 del firewall in uscita e di EMET e salvare punti di ripristino

7.7.2 - LINUX
Le solite cose da 15 anni a questa parte piu' o meno:
1) patch patch patch!!! sempre comunque e quantunque
2) disabilitare i vecchissimi servizi di inetd e xinetd (telnet, in.ftp)
3) disabilitare funzioni di rete inutili editanto sysctl.conf e reboot
   net/ipv4/icmp_echo_ignore_broadcasts = 1
   /proc/sys/net/ipv4/conf/all/log_martians = 1
   net/ipv4/tcp_syncookies = 1
   net/ipv4/icmp_ignore_bogus_error_responses = 1
   net/ipv4/conf/all/accept_redirects = 0
   net/ipv4/conf/all/send_redirects = 0
   net/ipv4/conf/all/forwarding = 0
   net/ipv4/conf/all/rp_filter = 1
   net/ipv4/conf/all/accept_source_route = 0
4) stampanti remote: cups (/etc/cups/cupsd.conf)
   Listen 127.0.0.1:631
        <Location />
      Order Deny,Allow
      Deny From All
      Allow From 127.0.0.1
     </Location>
5) eliminare servizi inutili:
   ps axu vi dice quelli che sono attivi
   netstat -nap vi dice le porte aperte
   lsof -i vi dice pure le porte aperte
   lsof vi dice tutti i processi sul sistema
   runlevel vi dice in che runlevel siete
   ls -l /etc/rc.d/rc.RUNLEVEL/S* vi da' la lista di quelli che partono
     nel vostro runlevel. cancellare (tanto sono link) quelli che non
     servono.

(su redhat esiste il chkconfig e il comando service ma e' uguale)

Esempio di robe quasi sicuramente inutili: nfs
se un servizio e' proprio necessario proteggerlo tramite il firewall
locale (iptables) consentendo l'accesso solo a certi ip o certe reti

6) default password policy /etc/login.defs
7) cambiare la validita' delle password con chage:
   chage –M 60 –m 7 –w 7 username (M giorni minimi, m giorni massimi,
   w numero di giorni dell'avviso di scadenza)
8) eliminare la shell di login al root (/sbin/nologin)
9) utilizzare sudo (invece che su) se ci sono piu' utenti su una macchina
10) disabilitare accesso privilegiato remoto (non solo root)
   /etc/security/access.conf aggiungere:
   -:wheel:ALL EXCEPT LOCAL

11) solo root accede al cron:
   cd /etc
   rm -f cron.deny at.deny
   echo root > cron.allow
   echo root > at.allow
   chown root:root cron.allow at.allow
   chmod 400 cron.allow at.allow
12) disabilitare messaggi informativi di banner
   Per esempio invece di mettere "Benvenuto a Linux Debian 0.1.2 kernel
   0.9.28 vuoi sapere anche la mia CPU la mia RAM e il mio disco?"
   "Authorized Access Only" per esempio. Metterlo in
   /etc/motd
   /etc/issue
   /etc/issue.net
   gdm.conf
13) installare logwatch; dentro /etc/cron.daily/00logwatch inserire:
    /usr/sbin/logwatch --output mail --mailto MIAMAIL@XX --detail high
14) valutare la possibilita' di installare un hardenizzatore
   automatico: 'harden' su debian
   'bastille UNIX' per tutti: http://bastille-linux.sourceforge.net/
15) chrootare il piu' possibile tutti i servizi (shell, apache, ftp,
    DNS-Bind etc etc)
16 PARANOID) valutare l'utilizzo di Selinux

Alcuni servizi principali:
A) OpenSSH server: /etc/openssh/sshd_config
   Protocol 2
   PermitRootLogin no
   PermitEmptyPassword no
   Banner /etc/issue
   Ingnore Rhosts yes
   RhostsRSAAuthentication no
   HostbasedAuthentication no
   LoginGraceTime 1m o meno
   SyslogFacility AUTH
   AllowUser pippo pluto topolino
   DenyUser minnie paperino gambadilegno
   MaxStartups 10 o meno

   Valutare se e' fattibile cambiare porta per ssh, ci evitiamo
   milioni di scanport!
   Port 22222 per esempio

B) Apache httpd
1) parmessi sui file delle cgi:
   chown root directory_cgi
   chmod 755 directory_cgi
2) rimuovere la direttiva Indexes
3) rimuovere la UserDir
4) informazioni sul server: disabilitare al massimo:
   ServerTokens Prod
   ServerSignature Off
   TraceEnable Off
   Header unset ETag
   FileETag None
   in php.ini
   expose_php = Off
   display_errors = Off
   track_errors = Off
   html_errors = Off

5) AllowOverride None
6) Rimuovere la versione 1 del protocollo HTTP
   RewriteEngine On
   RewriteCond %{THE_REQUEST} !HTTP/1\.1$
   RewriteRule .* - [F]
7) Disabilitare SSL v.2
   SSLProtocol –ALL +SSLv3 +TLSv1
8) rimuovere moduli indesiderabili se possibile (Esempio: proxy_mod)
9) ovviamente non farlo correre come root (ma il default gia' da tempo
   e' cosi' a meno che uno non voglia sbagliare proprio apposta)
10) mod_headers: configurare
   Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure
   Header always append X-Frame-Options SAMEORIGIN
   Header set X-XSS-Protection “1; mode=block”
11) novita': valutare l'installazione di mod_security; fa funzionare
Apache
   come un firewall, ma bisogna leggere comunque i log
12) mod_evasive: previene attacchi DDoS, HTTP brute force

C) ftp-server
   vsftp: chroot e possibilmente disabilitare ftp anonimo

D) MTA locale (redireziona verso il cerver centrale)
   update-inetd --disable smtp
   Installare postfix
   in main.cf mettere: inet_interfaces = localhost
   oppure installare nullmailer o ssmtp
E) MTA di Istituto
1. non farlo correre da root
2. cambiare i permessi e ownership ai file:
   chmod 755 /etc/postfix
   chmod 644 /etc/postfix/*.cf
   chmod 755 /etc/postfix/postfix-script*
   chmod 755 /var/spool/postfix
   chown root:root /var/log/mail*
   chmod 600 /var/log/mail*
3. Suggerimenti da inserire in main.cf
   inet_interfaces = 192.168.1.1 solo quella che vogliamo che risponda
   mynetworks = 10.0.0.0/16, 192.168.1.0/24, 127.0.0.1 trusted networks
   myorigin = example.com
   mydomain = example.com
   relay_domains = example.com
   Contro il DoS:
   default_process_limit = 100
   smtpd_client_connection_count_limit = 10
   smtpd_client_connection_rate_limit = 30
   queue_minfree = 20971520
   header_size_limit = 51200
   message_size_limit = 10485760
   smtpd_recipient_limit = 100
   smtpd_helo_required = yes
smtpd_helo_restrictions = permit_mynetworks, permit_sasl_authenticated,
reject_non_fqdn_helo_hostname, reject_invalid_helo_hostname
strict_rfc821_envelopes = yes
smtpd_client_restrictions = permit_mynetworks, permit_sasl_authenticated,
reject_unknown_client_hostname, check_client_access mysql:/etc/postfix/
mysql-virtual_client.cf
smtpd_recipient_restrictions = permit_mynetworks,
permit_sasl_authenticated,
reject_unauth_destination, check_recipient_access mysql:/etc/postfix/

mysql-virtual_recipient.cf, reject_unknown_recipient_domain
smtpd_data_restrictions = reject_unauth_pipelining
smtpd_delay_reject = yes
da postfix 2.8 in poi:
postscreen_greet_action = enforce

in master.cf:
```
smtp      inet  n       -       n       -       1       postscreen
```

4. bloccare a livello di router di accesso il traffico SMTP in uscita
   (proto TCP and port 25) che non e' generato dal'MTA istituzionale
   Chi vuole mandare e-mail con la propria macchina deve comunque passare
   dal server centrale (che avra' anche antispam, antivirus etc etc)
5. forzare gli utenti a scegliersi delle password "decenti"

Applicazioni lato server:
joomla, wordpress, drupal, php, java
Per tutti vale la solita regola: tenerli sempre aggiornati all'ultima
versione. Non e' sempre facile perche' i componenti aggiuntivi spesso
non funzionano sulle versioni nuove e bisogna aspettare loro.
Stessa cosa per il php/java
Controllare bene la lista dei componenti aggintivi necessari e rimuovere
quelli che non servono, aiuta ad eleminare un po' di codice passibile
di injection.
sicuramente aiuta anche modificare i comuni parametri di connessione al
db o parametri speciali:

1. modificare la username dell'utente super privilegiato (solitamente
   admin); mettere delle password impossibili
2. per CMS: modificare i prefissi delle tabelle nel db: per esempio
   le tabelle di joomla si chiamano tutte: jos_
   Inventatevi un altro prefisso: cof_

Il consiglio che si puo' dare e' seguire bene i siti che segnalano
le vulnerabilita' dei sistemi utilizzati, quando possibile aggiornare,
quando non e' possibile si dovrebbe disabilitare la funzione vulnerabile
non c'e' altra via di scampo purtroppo

Microsoft IIS
- Non installarlo su un domain controller
- non attaccarlo alla rete fino a quando non e' finita la procedura
  di hardening
- non installare stampanti
- utilizzare due interfacce di rete, una per il server web, una per
  la configurazione/gestione
- lanciare IISLockdown
- installare e configurare URLScan
- disinstallare il guest account
- creare un anonymous account per ogni virtual host, senza permessi di
  scrittura sull'albero html, ne' di lettura al di fuori del proprio
  virtual host. Non dare permessi di esecuzione alle command line
- configurare ASP.NET con meno privilegi possibili
- non creare piu' di due utenti del gruppo amministratori, loggarsi
  come amministratore solo da locale
- installare la DocumentRoot in un disco fisico differente dal sistema
  operativo
- mettere i log in un altro disco ancora
- disabilitare SEMPRE il default site e crearne uno nuovo da scratch
- restringere il gruppo Everyone togliendo accesso a \windows\system
- rimuovere gli esempi: \WINNT\Help\IISHelp, \Inetpub\IISSamples
- rimuovere lo strumento di configurazione remoto:
  \WINNT\System32%#92;Inetsrv\IISAdmin

- rimuovere tutti gli share, anche quelli di sistema
- disabilitare "parent path"
- rimuovere le seguenti virtual directory: IISSamples, IISAdmin, IISHelp and Scripts.
- rimuovere la MSADC virtual directory
- togliere scrittura ed esecuzione all'utente web in tuttii virtualhost
- rimuovere le FrontPage Server Extensions
- rimuovere la IIS Internet Printing virtual directory
- mappare come errore 404 (404.dll) le seguenti estensioni: .idq, .htw, .ida, .shtml, .shtm, .stm, idc, .htr, .printer
- Mappare dentro Machine.config le estensioni ASP non necessarie come HttpForbiddenHandler
- rimuovere filtri ISAPI non necessari
- proteggere e restringere gli accessi a %systemroot%\system32\inetsrv\metabase.bin
- restringere IIS Banner information
- Machine.config:
  - Quello che non vogliamo usare proteggiamolo con HttpForbiddenHandler
  - i moduli che non usiamo togliamoli (HttpModules)
  - disabilitiamo il tracing: <trace enable="false"/>
  - togliamo il debug dei compilatori (obbligatorio in produzione!) <compilation debug="false" explicit="true" defaultLanguage="vb">

Applicazioni lato client
Firefox:
Le debolezze maggiori stanno sulla gestione del javascript, iFrame, gif malevole) e nell'installazione selvaggia di componenti aggiuntivi, che aggiungono bug al sistema (java, flashplayer, shockwave)
Tutti questi oggetti sono autorizzati ad eseguire codice sulla macchina, e se son bacati un attaccante scrive sulla macchina quello che vuole

Il consiglio che si puo' dare e' tenere il browser sempre all'ultima versione, anche dei plugin

Inoltre si posson installare i seguenti plugin di sicurezza:
 NoScript
 AdBlock Plus
 WOT (web of trust) (adesso c'e' anche per IE)

Una cosa che possiamo fare per beccare i JAVA malevoli:
bloccare a livello di firewall o di proxy in uscita tutte le richieste HTTP con la stringa Java User-Agent

Abrobat Reader:

stessa cosa dei browser: esegue i javascript!
quindi va protetto, oltre che tenuto aggiornato all'ultima versione

nelle preferenze:
dentro javascript disabilitare "Enable Acrobat Javascript"
dentro Security Enhanced - Protected View: All Files
dentro Security Enhanced - Create Protected Mode Log File
dentro Security Enhanced - disabilitare "automatically Trust Sites from my Win OS Security Zones
dentro Trust Manager - disabilitare "Allow Opening of non-PDF file attachment"

dentro Trust Manager - Internet Access from PDF outside the web browser - change settings - selezionare "Block PDF file access to all web sites"

DISPOSITIVI:
stampanti, scanner, fax, router wifi
Ormai hanno tutti una scheda di rete incorporata per poter essere gestiti da remoto. Mediamente (a parte i router che possono anche essere di vendor "famosi" tipo Cisco, fortinet e avere un proprio SO) hanno un sistema operativo linux embedded degli anni 90, con tutti i buchi di sistema che si porta dietro da 15 anni a questa parte.
Il problema e' che essendo embedded, il sistema non si puo' patchare, e il costruttore difficilmente rilascia dei firmware che si occupano di chiudere i buchi di sicurezza (vale la pena comunque controllare periodicamente se ci fossero). La strategia e' disabilitare TUTTO

I principali problemi che danno questi oggetti sono DDoS e DoS, sono bucate
e dentro viene installato software di scanning, SPAM. Sono molto preoccupanti
perche' ce ne sono sempre di piu' e le tecniche di sfruttamento sono sempre piu' fini e sofisticate perche' rende veramente un sacco di soldi sfruttarle.

1- hanno SNMP (v.1 del protocollo) attivo per fare statistiche da remoto
   delle pagine stampate etc etc. Hanno abilitato la default community
   'public' in lettura a volte anche in scrittura, a volte con una
   password sciocca ("public" o "admin")
   VA DISABILITATO SNMP (oppure se proprio lo vogliamo, va configurata
   una community piu' protetta)
2- hanno NTP in una versione paleolitica che risponde a qualsiasi tipo
   di query malevola.
   VA DISABILITATO NTP
3- hanno un MTA installato per mandare mail di log all'amministratore
   e' vecchio e bucato
   crede di essere l'mta istituzionale e FA DA RELAY
   non fa nessun controllo sul mittente, contenuto, limitazioni di
traffico
   VA DISABILITATO SMTP
4- hanno HTTP anziano (tipo apache 1.x) e bucato
5- hanno l'interfaccia amministrativa via HTTP TERRIFICANTEMENTE debole:
   a. password di accesso inesistenti (o di default o indovinabili)
   b. php o java o quello che e' super vecchio/bucatissimo ai cross
   site scripting
6- hanno OpenSSL obsoleto con certificati bucati/bucabili
7- di conseguenza anche se l'interfaccia di gestione fosse in HTTPS
   sarebbe ugualmente una porta spalancata per l'hacker
   ELIMINARE interfaccia HTTP e HTTPS
8- hanno I TCPSimpleService...
   TELNET (TCP port 23)
   CHARGEN TCP e UDP port 17
   ECHO TCP e UDP port 9
   DISCARD TCP e UDP port 19
   come si fa nel 2014 ad avere il telnet?
   ELIMINARLI!
9- anche se avessero ssh sarebbero bucati per la debolezza intrinseca
   del sottostrato Openssl (e ultimamente ne sono stati trovati assai
   di buchi su openssl!)
   DISABILITARE SSH

Ultimo consiglio: per evitare che un eventuale hackervi faccia un disegno sulla vostra stampante, ma soprattutto faccia danni ben piu' grossi, cercare di tenere questi dispositivi su una rete apposita, accedibile solo

da reti apposite. Bloccate il traffico in uscita, specialmente SMTP, UDP e perdinci i SimpleTCPServices: nel linux sono stati eliminati di default 15 anni fa. Se questi linux embedded li hanno ancora abilitati significa che sono piu' vecchi di 15 anni... meditiamo gente

password deboli:
E' uno dei principali sistemi per entrare e sfruttare la nostra rete purtroppo. Soprattutto mi riferisco ad account di posta bucati che, non solo leggono tutta la posta e ottengono tantissime informazioni sulle persone (in modo da mandare spam mirato oppure accedere a cose piu' remunerative tipo il conto corrente o la carta di credito).
Il problema GRAVE e' che spediscono anche posta indesiderata a tutto il mondo

Consigliamo di educare il proprio personale all'utilizzo di password forti.

Per esempio invece del nome del figlio non e' necessaria una password tipo: "fkdDeekgYT993785.GGSDsf.--è9$(£/%ggT5yHH" ... basterebbe mettere

tommasopesava3.700g
alle17usciro'diqua

per esempio... oppure prendere le iniziali di una frase che si ricorda bene, tipo la propria canzone preferita:

Una Rotonda Sul Mare, Il Nostro Disco Che Suona;
Vedo Gli Amici Ballare: Ma Tu Non Sei Qui Con ME!

diventerebbe:

Ursm,Indcs;Vgab:MtnsqcM!

Basta aggiungere qualche numero e siamo a posto!
cioe' non importa che le password siano impossibili da ricordare, ma devono essere lunghe, almeno 15 caratteri, con qualche numero e/o segno di interpunzione.... anche semplici

Fattore umano:
un altro fattore di estrema debolezza e' il lato umano, con le sue proprie vulnerabilita'

Un esperimento fatto di recente consisteva nel mandare una mail di phishing a tutti gli utenti di una organizzazione.

La mail era scritta piuttosto male e chiedeva di cliccare un link e mettere nella pagina il proprio indirizzo mail e la propria password.
Era scritta piu' o meno cosi' (cito liberamente e aggiungo a mia fantasia quando non ricordo bene, giusto per far capire che era scritta proprio male!)

Distinta utente,
prego vedere me no come spam. Tuo problema posta elettronica si risolve cliccando sul mio sito e mettere tua email e dopo anche password.

Cliccare qui

Il link puntava ad una pagina web, appositamente su un dominio completamente estraneo alla struttura. L'utente si trovava una pagina bianca senza nessun logo che ricordasse la propria amministrazione

(ne' altro) con un form dove inserire mail e password.
e' SPAVENTOSO il numero di persone che hanno messo la propria mail e password su quel sito.

Cosa si impara e come ci si difende?
Si impara che l'utente se non e' allenato ed educato e' portato a cliccare ovunque ci sia un link cliccabile.
e' necessario informare, educare, instillare nell'utente un po' di paranoia per la propria sicurezza. Bisogna insegnargli anche come leggere le mail e come accorgersi se c'e' qualcosa che non va.
Bisogna descrivere bene i rischi a cui si va incontro, sia per il furto di dati personali, sia per la struttura a cui l'utente appartiene.

Il consiglio e' prevedere per ogni utente/dipendente/docente una breve sessione riservata alla tutela dei propri dati e della sicurezza della propria istituzione, almeno una volta all'anno. Come si fa per la 626 in cui si fa un refresh delle informazioni (e volendo anche qualche esercitazione).
Una cosa leggera e divertente, ma anche un po' spaventosa.

Mobile e SMART Mobile
il numero di telefonini (smart) + tablet e' 10 volte il numero di PC + server nel mondo: la fetta di mercato e' 10 volte piu' ampia.
Investimento pazzesco nella ricerca per diffondere il BADware via mobile che fortunatamente ha problemi di spreading del software malevolo:

- deposito di applicazioni bacate con il malware su google play/Baidu App Store; mediamente ci vogliono 15 giorni prima che si accorgano che l'applicazione e' malware e la tolgano. Ultimamente sia google che baidu hanno inserito delle sandbox che testano al volo le applicazioni che vengono caricate sul repository, ovviamente ultimamente il malware e' piu' furbo e si accorge di quando e' eseguito su una sandbox e fa finta di comportarsi bene

- utilizzo app store di terze parti - anche utilizzo di ROM di terze parti (moddate per esempio)

- SMS - se una app in fase di installazione chiede di accedere agli SMS significa che puo' leggere tutti gli SMS... cosa succede se il telefono e'
sotto controllo mentre si sta facendo un acquisto con carta di credito e la banca mi manda via sms il codice da utilizzare per la transazione?
E' lo stesso principio con cui si fanno i soldi su bitcoin, anche se il sistema e' diverso

- femtocelle (furto di SIM e relativo numero di telefono, il TAN della banca, furto di identita': il numero di telefono e' registrato con il codice fiscale di una persona; invio di SMS ulteriori per infettare i contatti con malware)

- QR code malevolo - QR che puntano a siti web col malware

- bluetooth - infezioni al volo

- twitter/facebook
- pubblicita' malevola dentro le applicazioni "buone" (clicki e vai su siti malevoli)

- whatsapp (Priyanka) - non fa nulla di male, a parte togliere l'eventuale foto e cambiarti i nomi di tutti i contatti (rubrica, mail,

whatsapp stessa) in "Priyanka"... piuttosto fastidioso ma innocuo.
Ma se qualcuno si fa piu' furbo e scrive qualcosa di meno innocuo?
Chi puo' dirci che non esista gia' pero' non ne siamo a conoscenza?

- Il piu' pericoloso: USB!!!!
Windows infetta Android (Droidpak.A@Windows => Fakebank.B@Android)
Android infetta Windows (Claco.A@Android => SSucl.A@Windows)
basta attaccare il cavo USB

Statistichina
Nel secondo quadrimestre (3 mesi soltanto) del 2014 sono stati trovati:

727.790 pacchetti sugli store, di cui
 65.118 NUOVI BADware, di cui
  2.033 trojan su accessi alle banche
(fonte: securelist.com - Kaspersky)

Come ci si difende?
male... Possiamo dare dei consigli:

non parlo di telefoni moddati o rootati perche' il il discorso e' molto
piu' complesso. Parliamo dei telefoni/tablet "normali"

- evitare di stare in rete (internet) quando non serve
- utilizzare solo gli app store ufficiali
- controllare bene quando si installano applicazioni gratuite (un prezzo
  da pagare c'e' SEMPRE!).
- Verificare sempre, prima di installare, le recensioni
dell'applicazione,
  non solo quelle dello store ma anche sul web in generale
- leggere sempre con molta attenzione la lista dei dati a cui l'app
  chiede di accedere
- evitare di installare applicazioni che accedono agli SMS se non
  strettamente necessarie
- evitare di installare app che richiedono per forza il collegamento
  internet per motivi incomprensibili: per esempio se installo un
programma
  che mi fa da agenda, o un lettore di ebook non ritengo necessario che
  per funzionare debba per forza stare attaccato alla rete

IPV6:
Un consiglio mio personale, che puo' non rispecchiare le visioni/opinioni
del mio datore di lavoro: visto che al momento attuale non e' urgente
il passaggio a IPV6... PERCHE' tenerlo/installarlo/veicolarlo? :)

Vulnerabilita' e Attacchi:
Di default il protocollo e' implementato per aumentare lo spazio di
indirizzamento, senza minimamente preoccuparsi della sicurezza.

DISCLAIMER: il protovollo IPv6 non e' ancora nella sua versione stabile
e standardizzata, e' implementato su alcuni RFC che sono ancora in stato
di DRAFT. Le informazioni sotto riportate quindi si riferiscono alla
situazione attuale (giugno 2014). Resta inteso che alcune problematiche
possano essere risolte (ed e' auspicabile) nelle versioni successive
dei DRAFT o dell'implementazione del protocollo stesso.

le vulnerabilita' sono:

- Tutte quelle dovute alle nuove fantastiche features di IPv6
  (elenco sotto)

- IPv6 ESISTE anche se la propria rete non veicola o non supporta IPv6
    * e' installato e auto-configurato di default su Windows, Linux
- Tutte le vulnerabilita' di IPv4 (escluso un paio di casi particolari)

Vulnerabilita' introdotte dalle features di IPv6:

1) Extension header
  * Router Header Type 0: DoS sul router
  * Router Alert Option: impatta molto sulle performance del router

2) Frammentazione
  * TCP SYN DoS di frammentazione (evitabili con IPv4)
  * a seconda del tipo di riassemblamento analizzando il pacchetto riassemblato, ho informazioni sul sistema operativo (fingerprinting)
  * essendo la frammentazione un processo stateful, se utilizzata su un protocollo stateless (udp o icmp) puo' facilmente esser utilizzata per attacchi DoS

3) Flow label:
  * in IPv6 e' obbligatorio (sembra che questa obbligatorieta' sara' quasi certamente abbandonata nelle versioni successive dei DRAFT) che ogni pacchetto abbia la sua flow label, quindi sulla rete passano un numero esagerato di label con nomi differenti: il router che deve processare i pacchetti deve tenersi in memoria tutte le label dei pacchetti che fa transitare: si siede
  * inoltre e' facile forgiare pacchetti con una flow label data in modo da sfruttare il QoS a proprio vantaggio per quella label

4) Neighbor Discovery
Il Neighbor Discovery e' implementato per fidarsi di chiunque sulla proria rete locale. Se un malvagio installa malware su un qualsiasi PC, dove tutti i PC di default sono configurati per funzionare in IPv6, riesce in pochissimo tempo a formarsi una LAN totalmente IPv6 che puo' sfruttare a suo piacimento. Di seguito i principali attacchi che sfruttano
le debolezze del NeighborDiscovery protocol
  * Address resolution: attacchi spoofing duplicando le risposte al neighbor deection (mitigazione: Duplicate Address Detection)
  * router advertisement spoofing: qualsiasi PC sulla rete locale puo' annunciare se stesso come router (stessa storia del vecchio STP spoofing sugli switch degli anni 90), quindi iniettare un prefisso arbitrario e dopo mettere il router lifetime a 0 cosi' che il client non chiedera' mai aggiornamenti al router vero. (Mitigazione: mettere in mezzo una macchina che filtra e droppa annunci illegali)
  * flooding di tutta la LAN impersonandosi come router e mandando Routing Advertisements con vari prefissi; in questo modo tutti i client di una LAN sono obbligati a prendersi un indirizzo per ogni prefisso causando un bel dossone.

5) Redirect: basta mandare un ordine di Redirects per cambiare la configurazione del malcapitato client

6) Smurf: attacchi DoS implementando lo smurf in multicast: un attaccante manda un pacchetto spoofato con SRC=vittima all'indirizzo multicast, che risponde alla vittima e causa DoS.
Possibile mitigazione

  * impedire all'indirizzo multicast di rispondere
  * eventualmente (anche se e' contro l'attuale RFC) droppare i pacchetti con "unknown option"

Nonostante questo si devono comunque far passare i messaggi di "Packet too big" (per il path MTU discovery) quindi la potenzialita' del DoS tramite Smurf non si puo' eliminare
Per prevenire lo spoofing all'inizio era stato proposto nell'RFC di utilizzare IPSec, ma questo comportava lo scambio fisico delle chiavi prima della prima installazione del PC sulla rete, quindi non era fattibile. Adesso in RFC c'e' un sistema, chiamato SeND (Secure Neighbor Discovery): vengono generati degli indirizzi criptati associati alla chiave pubblica di un host cosi' i messaggi di neighbor discovery vengono scambiati su canali criptati, ma ancora non va bene perche' l'algoritmo RSA oltre che backdoorato e' molto dispendioso in termini di CPU necessaria alla crittazione/decrittazione quindi facilmente con SeND si generano DoS sul proprio router

7) Multicast Listener Discovery
e' il protocollo che informa la rete di quali sono gli indirizzi multicast, viene inviata dal router una query regolarmente a tutta la rete chiedendo chi e' che ascolta su indirizzi multicast.
Un attaccante puo' facilmente dichiarare di essere il query router: in IPv6 basta mettersi l'indirizzo piu' basso! :: (tutti zeri) per esempio e smettere di mandare le query: cosi' nessuno forwarda piu' ai multicast e genera DoS
Mitigazione
  * assegnare l'IP piu' basso al router
  * non assegnare l'IP piu' basso al router (altrimenti succedono altre cose spiacevoli)

  I due consigli precedenti sono volutamente contraddittori nel senso che uno mitiga certi aspetti del problema, mentre apre nuove brecce, l'altro mitiga altri aspetti, ma apre anche altre brecce. Per il momento questo problema, con questi RFC, non e' risolvibile

8) Tunnel
All'inizio tutti i router facevano passare ipv6 senza controllo: se i nostri router non sono di ultimo modello e' necessario che tutte le regole iptables siano applicate sia per IPv4 che per IPv6. Adesso sui router di ultima generazione il default e' droppare a livello di router IPv6, quindi, per far funzionare il v6 in un ambiente solo v4, e' stato inventato il tunneling. Il tunnelig c'e' sempre stato, ma e' utilizzato impropriamente dagli attaccanti per bypassare le politiche di sicurezza. Inoltre l'attaccante non deve fare molti sforzi per tirarsi su un tunnel: nei sistemi Windows di default la macchina quando si accende va a cercarsi
un indirizzo anche in v6, e se non lo trova, fa salire in automatico il tunnel. Ecco alcuni tipi di attacchi:
  * meccanismi automatici di tunneling (Taredo, ISATAP): l'attaccante manda un pacchetto v6 con sorgente spoofato e lo incapsula in v4; quando arriva a destinazione il tunnel lo spacchetta e lo processa e risponde con un pacchetto destinato alla vittima v6. Nessuno se ne accorge perche' il pacchetto v6 viene incapsulato in un tunnel v4.
  * Taredo: forgiando richieste assurde si creano loop infiniti (DoS)
  * tunnel in tunnel in tunnel [...]: tunnellizzare a matrioska o scatola cinese permette ad un attaccante di caricare eccessivamente i router e PC di una struttura e permette la frammentazione di pacchetti a piacimento.

Mitigazione: settare la variabile Tunnel Encapsulation Limit ad un

numero molto basso (1 o 2 massimo)

9) Address Space troppo grosso
Se il Neighbor Discovery protocol non e' configurato si avranno troppe richieste pendenti per tutti gli indirizzi non esistenti e per esempio durante un network scanning sulla LAN si provoca facilmente un DoS.
Mitigazione: filtrare e droppare ip non utilizzati e subnettare mantenendo il numero di host per subnet piuttosto basso.
Probabilmente l'RFC nuovo includera' delle direttive per ridurre lo spazio di indirizzamento di una subnet a una /124 o al limite una /64
Anche l'ultimo RFC su ICMPv6 mitiga la formazione di questi loop infiniti/richieste pendenti implementando la risposta di Destination Unreachable

10) Mobile network
Come per IPv4 (ma di piu' perche' IPv6 si autoconfigura ogni X minuti, qundi posso mandare delle configurazioni spoofate a mio piacimento) attaccarsi alla rete "aziendale" tramite propri mezzi (portatili, tablet, telefonini) IPv6 e' prono ad attacchi di man in the middle, hijacking, DoS
Mitigazione: IPSec

11) Privacy issue:
attualmente l'indirizzo a 128bit e' dato da una parte "di rete" e una parte generata dall'host, ad oggi l'indirizzo ethernet della scheda di rete. Monitorando l'ip e filtrando per indirizzo ethernet vedo tutti gli spostamenti di quella persona attraverso le diverse reti.
Mitigazione: MD5 hash dell'host, oppure DHCPv6 DUID

[...]

Conclusioni:
Aspetti importanti nella vita di tutti i giorni
 ** se si vuole avere una network IPv6 compliant non va bene la configurazione standard dei router (tutti), ma va implementata una configurazione ad hoc che tenga conto della topologia fisica e logica, lo spazio di indirizzamento, i servizi offerti, la loro posizione topologica, e la tipologia degli utenti finali.

Alcuni aspetti di basso livello (LAN e router) da configurare sono qua:
https://www.usenix.org/conference/woot14/workshop-program/presentation/ullrich

Se si decide di NON VOLERE IPv6 nella propria struttura
  ** volere NON e' potere:
TUTTI i PC, e tutti i sistemi operativi sono configurati per essere nativamente pronti all'utilizzo di IPv6. Appena su una macchina nuova viene configurato IPv6, automaticamente e silenziosamente il sistema assegna alle interfacce di rete anche un indirizzo v6 e tira su i servizi necessari al routing e tunneling di IPv6. (S)Fortunatamente solo Linux non tira su nessun tunnel v4 di default.

Questo significa che e' acceso di default. Se la rete non veicola IPv6 automaticamente Windows configura e tira su dei tunnel che incapsulano il v6 in v4. L'effetto finale e' che vengono totalmente bypassate le regole di filtering del firewall di windows (che riguardano sempre IPv4) ma spesso anche i NAT server e i router gateway, rendendo inutili un sacco di precauzioni gia' prese.

(eventualmente:)

Per disabilitare totalmente IPv6 su Windows:
Il sistema protestera' molto perche' e' considerato un servizio essenziale al funzionamento del SO stesso. Effettivamente e' vero, ma pur disinstallandolo in realta' non si sono sperimentati problemi di nessun tipo.

Nei servizi:
Disable IPv6
Disable IPv6 tunnel interfaces (servizio IPHelper)
Control Panel / Device Manager, View menu / Show Hidden Devices

Eliminare:
Wan Miniport IPv6 driver
Teredo driver
ISATAP driver
IPv6 ARP driver

Aggiungere questa chiave di registro:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
\DisabledComponents 0xFFFFFFFF

Disabilitare IPv6 su Linux
Il sistema e' distro-dipendente. In ogni caso questi comandi funzionano per tutti (a volte sono ridondanti)
Si assume che il kernel sia superiore al 2.6.28
1- GRUB
   grub v1: in menu. lst cercare la riga defoptions= e accodarci il parametro: defoptions=ipv6.disable=1 quiet
   grub v.2: dentro /etc/default/grub cercare GRUB_CMDLINE_LINUX mettere: GRUB_CMDLINE_LINUX="ipv6.disable=1"
   anche: GRUB_CMDLINE_LINUX_DEFAULT="ipv6.disable=1 quiet splash"
   rebootare o lanciare update-grub (se debian)
2- sysctl
   Creare il file /etc/sysctl.d/noipv6.conf e metterci:
   net.ipv6.conf.all.disable_ipv6=1 riavviare
   eventualmente in /etc/sysctl.d/bindv6only.conf
   commentare: # net.ipv6.bindv6only=1
3- sysctl alternativo
   in /etc/sysctl.conf mettere
   net.ipv6.conf.all.accept_ra = 0
   net.ipv6.conf.all.disable_ipv6 = 1
   net.ipv6.conf.default.disable_ipv6 = 1
   net.ipv6.conf.lo.disable_ipv6 = 1
   lanciare sudo sysctl -p o rebootare
4- moduli del kernel
   in /etc/modprobe.d/aliases
      togliere alias net-pf-10 ipv6
        aggiungere alias net-pf-10 off
                   alias ipv6 off
5- moduli del kernel alternativo
    echo 'blacklist ipv6' | sudo tee -a \
      '/etc/modprobe.d/blacklist.local' >/dev/null
      echo 'install ipv6 /bin/true' | sudo tee -a \
      '/etc/modprobe.d/blacklist.local' >/dev/null
      reboot

8 - DoS e DDoS mitigating
Ultimamente stiamo assistendo a numerosi e ripetuti attacchi DoS e DDoS sulla rete. I possibili motivi sono svariati: guerra fredda cibernetica, concorrenza sleale in campo commerciale, lotta fra bande criminali per

sottrarsi vicendevolmente le botnet, estorsione etc etc
Il DoS e' uno strumento flessibile e versatile per mettere sotto scacco molto facilmente qualsiasi oggetto della rete: persone, aziende, governi, istituzioni. E' veramente facile. E soprattutto e' estremamente disponibile
La rete sembra fatta per veicolare questi tipi di attacchi.

Lo strumento principale usato per far DoS e' il protocollo UDP. I vari sistemi non sfruttano le debolezze intrinseche del protocollo, che pure ne ha, ma usano programmi e servizi mal configurati che permettono l'abuso
dell'utilizzo del protocollo.

Vediamo i principali servizi utilizzati con le possibili soluzioni per mitigare o risolvere il problema:

- SimpleServices (principalmente la porta chargen UDP e TCP 19)
- NTP
- SNMP
- DNS

Vediamo i dettagli:

- SimpleServices: sono principalmente dovuti a stampanti o dispositivi "intelligenti" facenti parte della IoT.
  Principalmente vengono da sistemi linux vecchi e vengono lanciati in fase
  di boot tramite il demone /etc/init.d (o xinetd.d se sono piu' recenti)
  Se si puo' accedere a questi dispositivi con una shell (OBBROBRIO!) conviene stopparli direttamente sul dispositivo, commentando TUTTE le righe ("echo", "chargen", "telnet", "discard", "ftp", "finger" "tftp")
  Far ripartire il dispositivo.

Se questo non fosse possibile e' auspicabile tenere questi apparati dietro un firewall/NAT che filtri tutti questi servizi. Meglio sarebbe mettere un filtro a monte sul proprio router di frontiera droppando tutti i pachetti TCP e UDP con src e dst port 7, 9, 13, 19, 21, 23
Diciamo di bloccare tutte le porte da 1 a 21 e la 23.

E' importante bloccarlo in uscita perche' e' in uscita che fanno il DoS. In questo caso e' piu' importante bloccarlo in uscita che in entrata.

- NTP
il Network Time Protocol e' tornato recentemente di moda perche' e' stata scoperta una feature che lo rende molto versatile per effettuare DoS sulla rete. E' il piu' pericoloso per una rete perche' ha un fattore di amplificazione anche di 4000 volte in alcuni casi: se non configurato ntpd risponde di default ad una piccola query con output molto verboso, dell'ordine anche di 4000 volte il pacchetto di ingresso: se 100 macchine mi fanno una query ntp per i 100 pacchetti UDP ricevuti ne rispedisco alla vittima circa 400.000.. e' facile saturare la banda

Attenzione: con questi enormi fattori di amplificazione e' facile saturare
anche la propria banda, non solo quella della vittima, quindi dobbiamo assegnare una priorita' forte a questo problema.

Il grosso del problema riguarda i router, poi le macchine linux che per aggiustare l'orologio invece che usare un ntp-client installano un ntp-server, poi comunque anche windows e soprattutto dispositivi e

stampanti

Sarebbe buona norma ciclicamente fare dei test sulla propria rete di questo tipo:

```
ntpq -c rv IP
ntpdc -c sysinfo IP
ntpdc -n -c monlist IP
```

con un script bash si piu' facilmente scansionare tutta la rete e calcolare
il rapporto di amplificazione per vedere se una macchina e' vulnerabile.
In questi casi si rimedia cosi':

Se la macchina e' un router:
- disabilitare ntp
- configurare ACL per far passare solo pacchetti NTP verso server "reali" nel mondo esterno (INRIM, Apple per esempio).. droppare qualsiasi altro pacchetto che non va verso questi server buoni.

Esempio CISCO iOS:

```
! Core NTP configuration
ntp update-calendar             ! update hardware clock (certain hardware
only, i.e. 6509s)
ntp server 192.0.2.1            ! a time server you sync with
ntp peer   192.0.2.2            ! a time server you sync with and allow
to sync to you
ntp source Loopback0            ! we recommend using a loopback interface
for sending NTP messages if possible
!
! NTP access control
ntp access-group query-only 1   ! deny all NTP control queries
ntp access-group serve 1        ! deny all NTP time and control queries
by default
ntp access-group peer 10        ! permit time sync to configured
peer(s)/server(s) only
ntp access-group serve-only 20  ! permit NTP time sync requests from a
select set of clients
!
! access control lists (ACLs)
access-list 1 remark utility ACL to block everything
access-list 1 deny any
!
access-list 10 remark NTP peers/servers we sync to/with
access-list 10 permit 192.0.2.1
access-list 10 permit 192.0.2.2
access-list 10 deny any
!
access-list 20 remark Hosts/Networks we allow to get time from us
access-list 20 permit 192.0.2.0 0.0.0.255
access-list 20 deny any
```

Oppure configurare NTP autentication via md5:

```
! general NTP and clock status
show ntp status
! lists synchronization details with configured peer(s)/server(s)
show ntp associations [detail]
! shows or logs detailed NTP messages/packets
```

JunOS:

```
system {
    ntp {
        authentication-key [key-id] type md5 value "[pass-phrase]";
        trusted-key [key-id];
        /* Allow NTP to sync if server clock is significantly different
than local clock */
        boot-server 192.0.2.1;
        /* NTP server to sync to */
        server 192.0.2.1;
        server 192.0.2.2 key [key-id] prefer;
    }
}
from {
    source-address {
        0.0.0.0/0;
        /* NTP server to get time from */
        192.0.2.1/32 except;
    }
    protocol udp;
    port ntp;
}
then {
    discard;
}
```

Macchine HOST (unix)
in /etc/ntpd.conf

```
# by default act only as a basic NTP client
restrict -4 default nomodify nopeer noquery notrap
restrict -6 default nomodify nopeer noquery notrap
# allow NTP messages from the loopback address, useful for debugging
restrict 127.0.0.1
restrict ::1 (se si vuole ipv6)
# server(s) we time sync to
server 192.0.2.1
server 2001:DB8::1
server time.example.net
```

e mettere iptables:

```
-A INPUT -s 0/0 -d 0/0 -p udp --source-port 123:123 -m state\
    --state ESTABLISHED -j ACCEPT
-A OUTPUT -s 0/0 -d 0/0 -p udp --destination-port 123:123 -m state \
    --state NEW,ESTABLISHED -j ACCEPT
```

NOTARE: questo problema viene veicolato anche su IPv6, quindi se si mettono i filtri vanno messi anche per IPv6

- SNMP

Protocollo di visualizzazione dello stato di oggetti in rete ed eventualmente modifica di alcuni parametri. Anche questo ultimamente e' sfruttato sulle stampanti, ma in ralta' sta ovunque, soprattutto in apparati hardware non molto intelligenti, ma che devono essere gestiti (router stessi, SAN, NAS, SWitch FC etc etc)

In questo caso si parla impropriamente di DoS, in quanto il problema generato dipende dal normale funzionamento di SNMP:
Cara scheda di rete, mi dici per favore le tue caratteristiche?
E quella risponde elencando IP, Ethernet Address, tipo di media utilizzato, quanti chip integrati ha, la descrizione e le caratteristiche

di tutti i chip che ha, la temperatura di lavoro, la velocita' delle ventole di raffreddamento...
... fattore di amplificazione molto molto alto

ad un piccolo pacchetto di richiesta corrisponde un volume della Treccani di pacchetti in uscita.

Cosa si puo' fare:
- disabilitare SNMP
- cambiare tutte le password della community di default (la password e' "public")
- bloccare sul router di frontiera tutto SNMP e abilitare solo quegli IP che possono accedere eventualmente (SNMP e' proto UDP and port 161)
- anche qua e' buona norma bloccare soprattutto il traffico SNMP in uscita

Regole sul router di bordo:
```
access-list 30 remark lasciamo passare l'SNMP abilitato E BASTA
access-list 30 permit 192.0.2.1
access-list 30 permit 192.0.2.2
access-list 30 deny any
!
access-list 40 remark idem in uscita
access-list 40 permit 192.0.2.0 0.0.0.255
access-list 40 deny any
```

- DoS DNS
Questi DoS accadono perche' i nostri DNS sono di default configurati per essere troppo gentili con gli estranei.

Arriva un estraneo e chiede:
- Caro DNS, mi diresti a che ip corrisponde l'host tanto.non.esisto.pappappero?

(dig @mio_dns dominio.inesistente)

Il DNS configurato male risponde:
caro amico, io proprio non lo so, perche' non sono aitoritativo per quel dominio, pero' siccome mi sei simpatico ti do' l'elenco dei server che potrebbero essere autoritativi e faccio io a loro la richiesta per te e la risposta e' NXDOMAIN. E ti lascio anche le statistiche del tempo che ho impiegato a fornirti una risposta, sono bravo eh

Al solito, la risposta e' mezzo volume della Treccani

Se non altro questo problema ha una soluzione rapida e indolore (almeno per le macchine con ISC Bind sia linux che windows)

SOLUZIONE FACILE per DNS ISC Bind (linux e Windows)
Si svolge in 2 passi:
1. definire chi e' la propria rete interna abilitata a far richieste al DNS
2. aprire le query ricorsive e la consultazione della cache DNS solo a quelle reti li'

Dentro named.conf
1.
```
acl "internal" { localhost; localnets; 192.0.2.0/24;
tutte_le_reti_interne; };
```

2. options {

```
            allow-query { any; };
            allow-recursion { internal; };
            allow-query-cache { internal; };
        };
```

Far ripartire ISC Bind

NOTA:
Per le macchine windows con DNS server di Microsoft dobbiamo purtroppo intervenire pesantemente sulla distribuzione degli IP della rete:

Il server DNS di Microsoft non permette la ricorsione condizionata, quindi non è possibile permettere la ricorsione per le richieste della rete interna ed impedirla alle richieste dalla rete esterna.

Le soluzioni possibili per arginare i danni causati dai DDoS possono essere le seguenti:

- limitare la banda: se il DNS Windows deve necessariamene essere visibile dall'esterno, si può limitare, tramite firewall, la banda di rete che può utilizzare;
- utilizzare BIND per Windows, identico nella configurazione a quello per Unix;
- utilizzare due server DNS, uno Microsoft che risponda soltanto alle richieste delle macchine della propria rete e ad Active Directory, con la ricorsione abilitata, e un altro che risponda soltanto alle query esterne per le macchine del proprio dominio di competenza e con la ricorsione disabilitata.
- In questo caso le configurazioni potrebbero essere:
  - server interno: nessun cambiamento, sia per il server sia per i client interni, che continuano ad usarlo come loro DNS;
  - server esterno:
    - ricorsione disabilitata;
    - contiene le zone dei domini di cui si è autoritativi.

Ovviamente bisogna comunicare al server DNS di livello superiore l'indirizzo IP del server esterno. In alternativa, forse piu' problematica,
si modifica l'IP del DNS server interno, anche su tutti i client, in modo che continuino a puntare a lui.

Apparati di rete
tenerli aggiornati sempre. E' risaputo che e' rognoso aggiornare un Cisco o un Juniper o un Fortinet o quello che e', ma va fatto.
Prendiamoci del tempo per controllare periodicamente se ci sono update e eventualmente per pianificare l'upgrade, avvertendo gli utenti di eventuali (ma dopotutto brevi) disservizi nel periodo di update.

ANCORA L'ANTI-SPOOFING!
Ad oggi molti router della rete GARR non hanno configurato le regole antispoofing per impedire i DoS. Sono regole che vengono dagli anni 90. Sono sempre quelle, non c'e' da aggiornare niente.
Controllate di avere le regole antispoofing sul vostro router di frontiera
oppure mettetele

La regola e' far uscire sull'interfaccia del nostro router che guarda internet SOLTANTO pacchetti con SRC appartenenti alle nostre reti. Ovviamente bloccare verso l'esterno anche le reti dette BOGUS, cioe' quelle assegnate a indirizzi privati da RFC. Inoltre bloccare le reti multicast (a meno di non dover fare il multicast) e la rete che windows

assegna alle macchine quando non "sentono" la rete o il DHCP:

```
access-list extended antispoofing
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.0.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 127.0.0.0 255.255.255.255 any
deny ip 224.0.0.0 15.255.255.255 any
deny ip 169.254.0.0 0.0.255.255 any
deny ip host 255.255.255.255
permit ip any mia.rete.mia.mia 0.0.0.255
```

OOPPURE ancora piu' facile:

```
access-list 150 permit ip mia.rete.mia.mia 0.0.0.255 any
access-list 150 deny ip any any log
interface serial0.1 (quella che guarda il GARR)
ip access-group 150 out
```

e' cosi' facile!

Spezzettare le reti interne:
assegnare sottoreti della propria rete a seconda dell'utilizzo che ne facciamo. Per esempio 10.0.1.0/24 sono i PC dei dipendenti, la 10.0.2.0/24 sono gli ospiti "cablati", la 10.0.3.0/24 sono gli ospiti in wireless ma con eduroam, la 10.0.4.0/24 sono gli ospiti in wireless con il captive portal IDEM, la 10.0.5.0/24 sono gli ospiti wireless generici, una rete diversa per la DMZ, una diversa per il management degli apparati di rete etc etc
Teniamo staccate queste reti fra di loro e non facciamo mai parlare le une con le altre (a livello gateway di ogni rete impostiamo dei filtri) teniamole anche fisicamente staccate, almeno a livello 2, tramite VLAN differenti sugli switch di collegamento e cerchiamole di farle passare da porte differenti (VLAN non trunked)

A livello logico, suddividendo il personale in interni ed esterni registrati,
(non parlo di esterni non registrati perche' per le AUP GARR e' necessario
sapere ad ogni ora a chi appartiene un IP della propria rete) una idea potrebbe essere:

Prima di tutto REGISTRARE gli utenti: quando un utente arriva con il telefonino nuovo (o un qualsiasi dispositivo) se vuole attaccarlo alla rete di istituto deve registrarsi, via cartacea o informatica, ricevere una breve informativa sui comportamenti non ammissibili o un opuscolo. Valutare l'opportunita' di registrare il MAC address dei dispositivi di un utente, in modo da fornire servizi soltanto tramite registrazione statica di un IP... altrimenti non si da' servizio. Questo e' utile anche per evitare che qualcuno utilizzi la rete invece che con il proprio dispositivo, con un piccolo router (wireless e non) e dia servizio ad altri sconosciuti. Se l'indirizzo hardware di un eventuale router wireless
non e' registrato nel nostro DHCP, non prendera' mai nessun indirizzo IP.
Valutare l'assegnazione di indirizzi IP statici basati sull'ethernet address (esempio il prof. X ha 10.0.1.37 sul PC dell' ufficio, 10.0.4.37 sul suo portatile, 10.0.100.37 sul telefonino). Ogni dispositivo potra' fare cose differenti sulla rete.

Non lasciare IP non utilizzati e non filtrati: se in una sottorete ci sono X indirizzi IP non utilizzati bloccate tutto il traffico da e per

questi IP: cosi' si evita che qualche utente smaliziato si metta un IP diponibile senza passare dal DHCP (e dalla registrazione)

La tipologia logica di accesso alla rete puo' suddividersi in:
- gli utenti interni (cioe' quelli che accedono con macchine dell'istituto
  configurate da noi) possono fare web, mail, SMTP, NTP sui server canonici
  possono accedere a qualche altra sottorete (servizi interni,
  intranet, DMZ)
- gli utenti esterni registrati (cioe' che hanno un proprio PC o tablet o
  telefonino) possono fare web, mail e SMTP. Se devono accedere a qualche
  sottorete valutare la possibilita' di dar loro un IP statico (privato)
  e creare delle regole opportune (ma minime) di accesso.
  Meglio sarebbe far loro usare una VPN, anche se fossero seduti accanto
  al server a cui devono accedere
- gli utenti di gruppi di ricerca (o assimilabili) che non possono usare
  i PC forniti dall'istituto (altrimenti diventano semplici "interni")
  oltre a web, mail, devono poter avere abilitati probabilmente strumenti
  di condivisione di cartelle e stampanti, e qualche possibile salto
  da una sottorete ad un'altra. Abilitare solo lo stretto necessario.
- Consiglio difficile da applicare: cercare di disincentivare l'utilizzo
  del mezzo proprio (come andare in missione con la propria auto) a favore
  degli strumenti forniti dall'Istituto (e' piu' sicuro, ci sono meno dati
  personali rubabili, puoi fare piu' cose senza restrizioni, puoi saltare
  in tutte le sottoreti etc etc)
- sconsigliare e disincentivare l'utilizzo di piattaforme esotiche (tablet
  e telefonini) per accedere a servizi interni. Puo' essere ammesso
  permettere ai dispositivi SMART di aggiornarsi e scaricarsi app e
  giochini, mandare whatsapp e scaricare/inviare mail, navigare in rete,
  ma non dovrebbero essere utilizzati per utilizzare i servizi
  di ateneo, tipo la procedura di contabilita' o simili.

Per tutti poi far valere le seguenti politiche:

Politiche ENTRATA
filtrare tutto in entrata (DROP di DEFAULT)
permettere soltanto ESTABLISHED
permettere dall'esterno soltanto l'ingresso verso i server o la DMZ

Politiche USCITA
se ogni pc o NAT fa il suo mestiere e filtra gia' a monte il traffico in uscita dovrebbe essere abbastanza pulito.
Ricordarsi comunque di:
- bloccare NTP escluso i server "canonici" (proto UDP and port 123)
- bloccare SNMP (escluso eventualmente macchine preposte al monitoraggio)
- bloccare SimpleServices (TCP and UDP port 1-21, 23)
- bloccare DNS in uscita escluso al nameserver istituzionale (UDP port 53)
- limitare UDP in uscita (per evitare i DoS e DDoS)
- limitare SMTP come numero di connessioni al secondo verso l'esterno
- pensare a politiche di limitazione di banda in emergenza:
  * quando il traffico grosso viene da una stessa sorgente
  * va su una stessa vittima
  * troppi pacchetti o troppi bytes al secondo

Policy di sicurezza

quello che ho appena detto sugli apparati di rete non e' volutamente completo perche' vorrei fare un discorso piu' ampio per cercare di riprogettare le policy di un Istituto o un campus universitario alla luce dell'utilizzo delle nuove tecnologie.

1- primo salto tecnologico: cambio di orizzonti
Prima c'e' stato il grosso impatto del wireless, che ha moltiplicato oltre misura il numero di macchine fisicamente attaccate alle nostre reti, ora l'impatto di telefonini e tablet che forse ne decuplica il numero... credo che tutto cio' ci abbia cambiato la vita o ce la stia per cambiare. In ogni caso come tutori di un certo livello di sicurezza dobbiamo modificare il nostro modo di pensare fino a ieri.
Il wireless ha portato un aumento di quantita' delle macchine attaccate alla rete, ma anche un allargamento dei nostri orizzonti: il perimetro della nostra rete da netto e chiaro e' diventato sfrangiato e impossibile da definire; i PC che si attaccano alla nostra rete sono stati in altre 1000 reti prima di noi e non sono puri come i PC dei dipendenti. I PC che hanno condiviso altre LAN hanno preso quello che c'era in tutte le altre LAN e non vedono l'ora di spargere quanto hanno appreso anche alla nostra LAN.

2- secondo salto tecnologico: cambio di prospettiva
Non solo, dobbiamo anche cambiare prospettiva: non possiamo piu' soltanto occuparci di difendere i server dalle compromissioni perche' non e' da li' che viene il male. Spero di aver dato un'idea del fenomeno: adesso dobbiamo occuparci principalmente dei client della nosta rete perche' il grosso del male sta tutto li'. Compromettere un apache aggiornato all'ultima versione con tutte le cose in regola e' piuttosto difficile se non impossibile, mentre compromettere una macchina windows con uno 0-day da 5$ e' facilissimo, direi banale, perche' a priori non c'e' nessuna forma di difesa.

3- terzo salto tecnologico: cambio di sistema difensivo
La nostra visione delle cose cambia anche dal punto di vista di quello da cui ci dobbiamo difendere: come abbiamo visto le minacce sono totalmente sconosciute, chiunque puo' entrare senza che noi abbiamo una minima idea di come abbia fatto (a volte non lo sa nemmeno lui come fa) quindi non possiamo piu' lavorare tentando di difenderci a priori; possiamo solo accorgerci che in qualche modo siamo stati compromessi
da come si comporta la macchina successivamente alla compromissione.
Per questo l'unica cosa che possiamo fare per difenderci e' contenere al massimo l'ambiente di un eventuale ospite nelle nostre macchine, perche' tanto prima o poi qualcuno che entra ci sara'.

4- quarto salto tecnologico: la rete siamo noi, non i nostri oggetti
Dobbiamo aiutare i nostri colleghi a capire che quello che fanno in rete potrebbe avere conseguenze spiacevoli prima di tutto per se stessi, poi per l'istituto dove lavorano, dobbiamo informarli di quello che c'e' sulla rete, dobbiamo istruirli su quali siano i comportamenti corretti, dobbiamo spiegargli a cosa portano i comportamenti scorretti. Dobbiamo aiutarli a scegliere il minor rischio possibile quando cliccano un link. Forse non lo sanno ma la rete sono loro, non tutti gli oggetti che si portano appresso

COSA FA GARR
1- Scansioni remote (soft penetration test)
SCARR: http://scarr.garr.it
e' un nessus server con licenza PRO, tutti i plugin installati a disposizione degli APM.

Chi ha un account SSO puo' chiedere l'abilitazione qua:
https://login.sso.garr.it/GarrSSO/module.php/selfregister/requestAccess.php?SP=SCARR

Chi e' apm e non ha ancora un account puo' farselo qua:
https://login.sso.garr.it/GarrSSO/module.php/selfregister

appena entrati si inserisce l'ip, gli ip, la rete o le reti da scansionare e il tipo di scansione. Poi di deve scegliere il tipo di scansione da effettuare, cioe' la lista delle vulnerabilita' che Nessus deve testare sulla rete indicata.

Quando SCARR ha finito viene mandato all'APM e ad uno o piu' indirizzi aggiuntivi il report per mail. Il report e' uno standard report di Nessus:
vengono indicate le vulnerabilita' in ordine di importanza, il CVE relativo alla vulnerabilita', informazioni aggiuntive e a volte alcuni suggerimenti di come risolvere la vulnerabilita'

2- Segnalazione incidenti di sicurezza: per voi saranno rognosi, ma grazie alle segnalazioni esterne siamo in grado di renderci conto del brutto della nostra rete, e noi ben felicemente vi giriamo gli incidenti di sicurezza

3- segnalazioni automatiche:
grazie ad un numero di sistemi di nomitoraggio inventati da GARR-CERT
grazie a due DarkNet su cui GARR-CERT ha messo HoneyPot di diversi tipi
e grazie a numerose e fruttuose collaborazioni internazionali di GARR-CERT,
siamo in grado di spedire una quantita' quasi decuplicata di segnalazioni di problemi su macchine della rete garr.
Vi chiediamo di prendere in carico le segnalazioni ed eventualmente avvertirci nel caso fossero falsi allarmi, in modo da raffinare le nostre tecniche.

4- impegno e collaborazione internazionale:
il GARR-CERT colabora e si impegna in seno alle principali associazioni di sicurezza internazionali (TF-CSIRT di TERENA, ENISA, Geant, DANTE), ma anche nazionali (Ministeri) a migliorare con ogni sforzo la situazione attuale, per questo contiamo sulla collaborazione di tutti gli APM e dei sistemisti e alla fine anche del personale che usufruisce dei servizi di rete

5- aiuto/consulenza: siamo "sul pezzo" nel momento del bisogno.
Scriveteci!
cert@garr.it