- il malware
- proteggere il computer
- il firewall
- il backup
- ottimizzare il computer

Il Malware

L'accesso indiscriminato ad internet espone l'utente al rischio di malware* di vario tipo e le conseguenze per la sicurezza e l'efficienza dell'azienda possono essere deleterie.

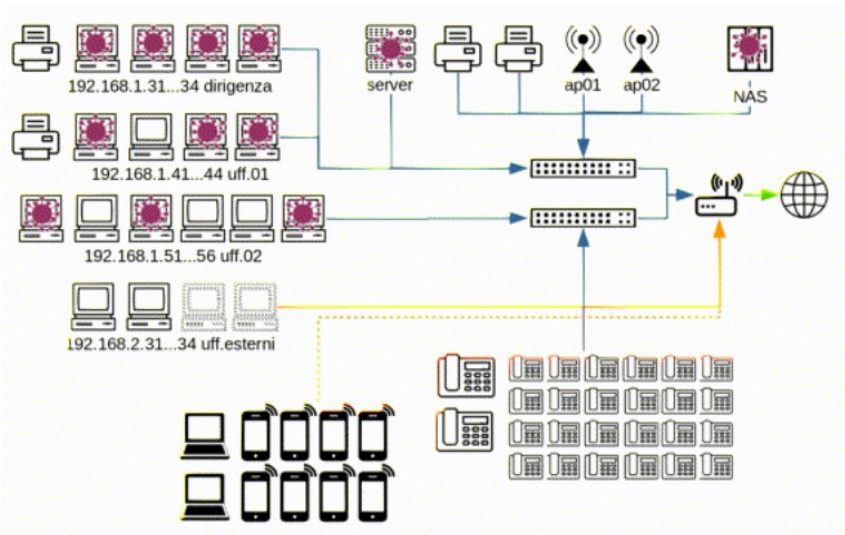
- rallentamento o blocco dei computer
- sottrazione di dati (documenti, password)
- criptazione dei dati a scopo di ricatto
- distruzione degli archivi
- uso indebito dei computer per fini criminali

**malicious software = programma dannoso*

Tipi di malware

- Virus: parti di codice che si diffondono copiandosi all'interno di altri programmi attivandosi quando il file infetto viene aperto.
- Worm: modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e rallentare il sistema con operazioni inutili o dannose.
- Trojan horse: software leciti che contengono istruzioni dannose eseguite all'insaputa dell'utilizzatore (Miner).
- Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato.
- Hijacker: causano l'apertura automatica di pagine web indesiderate.
- Rootkit: composti da un driver e da copie modificate di programmi presenti nel sistema. Vengono utilizzati per mascherare spyware e trojan.
- Adware: presentano all'utente messaggi pubblicitari durante l'uso, rallentando il computer.
- Keylogger: registrano tutto ciò che un utente digita su una tastiera o che copia e incolla.
- Ransomware: un tipo di Virus che cripta tutti i dati presenti su un disco a scopo di ricatto.

In una rete aziendale è sufficiente che un solo elemento venga contaminato per far si che l'intera rete venga compromessa.



Come il virus si propaga nella rete aziendale.

La cybersecurity

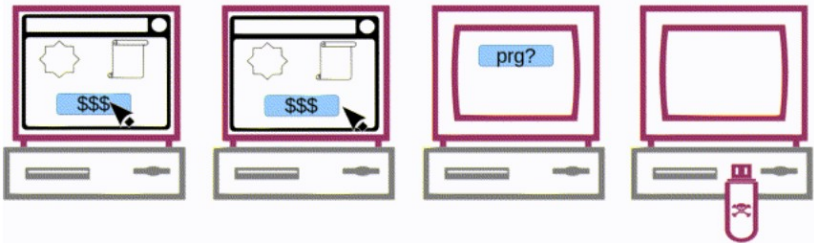
La sicurezza informatica è un compromesso tra protezione ed usabilità.
Si tende a raggiungere il compromesso più funzionale tra l'efficienza d'uso di un programma e la sua capacità di "sopravvivenza" ad attacchi esterni o ad errori più o meno critici.

> *The only truly secure system is one that is powered off*
> *(L'unico computer sicuro è quello spento)*
> *Eugene H. Spafford*
> *Ph.D Computer science at Purdue University (USA)*

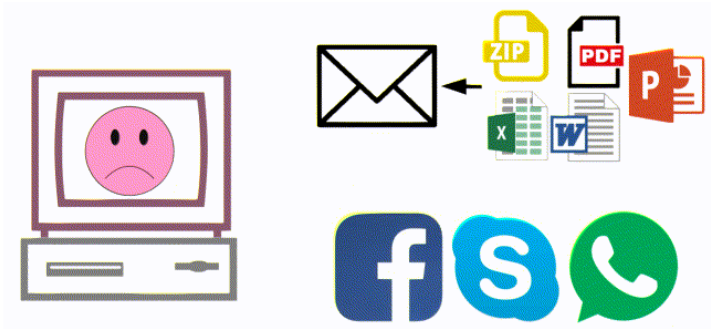
Come il malware entra nel pc

Oltre agli attacchi dall'esterno della rete ad opera di haker, solitamente è l'utente che agisce in modo più o meno inconsapevole scaricando il malware sul proprio computer.

1. Con un click su un pulsante/immagine di una pagina web.
2. Aprendo una pagina web, anche da una email.
3. Scaricando un programma da internet.
4. Inserendo una memoria usb infetta.

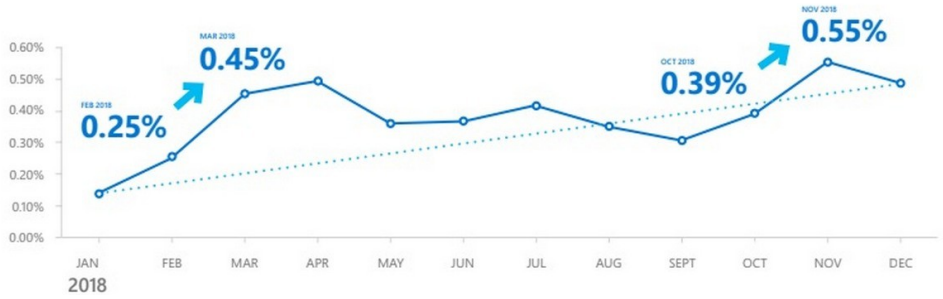


Ma anche aprendo allegati alle email (programmi, file compressi zip, documenti xls doc ppt pdf, immagini).
O scambiando file tramite i social (Facebook, Skype, Whatsapp).



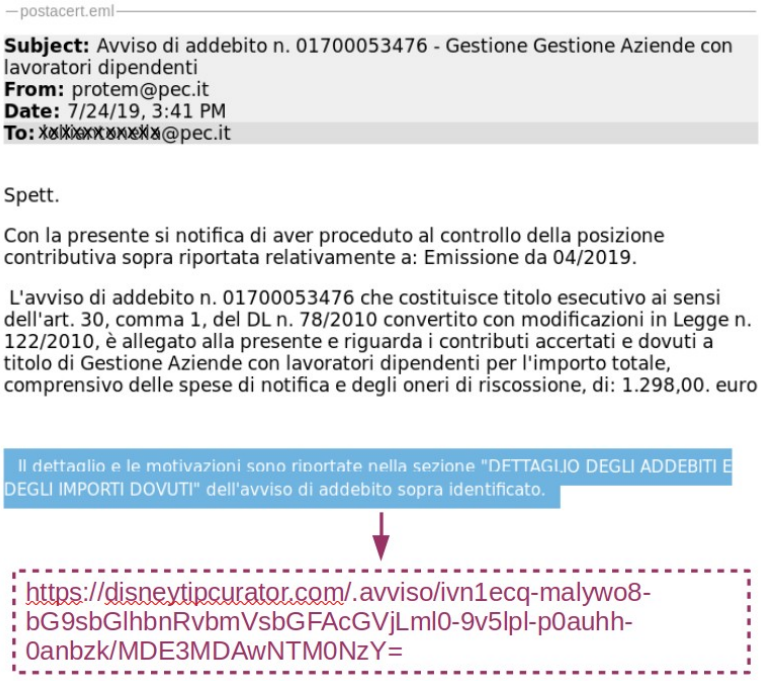
Il phishing

Il phishing è diventato in assoluto il metodo di attacco preferito dai cyber criminali, mentre i ransomware calano di popolarità lasciando il posto ai miner di criptovalute. (ricerca Microsoft).
In Italia i ransomware rappresentano ancora uno dei principali vettori d'attacco, specie verso aziende e uffici pubblici.



Il Phishing è una azione di inganno per convincere la vittima a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.
Sfrutta una tecnica di ingegneria sociale: un invio massivo di messaggi (email, sms, pec) che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi.
Il messaggio può non contenere codice maligno e quindi sfuggire ai controlli antivirus, ma un collegamento che rimanda ad una pagina web.
La pagina può contenere il malware che attacca il computer, oppure essere un clone del sito e chiedere all'utente di inserire le sue informazioni personali.

Di seguito un esempio di email phishing.


postacert.eml

Subject: Avviso di addebito n. 01700053476 - Gestione Gestione Aziende con lavoratori dipendenti
From: protem@pec.it
Date: 7/24/19, 3:41 PM
To: [redacted]@pec.it

Spett.

Con la presente si notifica di aver proceduto al controllo della posizione contributiva sopra riportata relativamente a: Emissione da 04/2019.

L'avviso di addebito n. 01700053476 che costituisce titolo esecutivo ai sensi dell'art. 30, comma 1, del DL n. 78/2010 convertito con modificazioni in Legge n. 122/2010, è allegato alla presente e riguarda i contributi accertati e dovuti a titolo di Gestione Aziende con lavoratori dipendenti per l'importo totale, comprensivo delle spese di notifica e degli oneri di riscossione, di: 1.298,00. euro

Il dettaglio e le motivazioni sono riportate nella sezione "DETTAGLIO DEGLI ADDEBITI E DEGLI IMPORTI DOVUTI" dell'avviso di addebito sopra identificato.

https://disneytipcurator.com/.avviso/ivn1ecq-malywo8-bG9sbGlhbnRvbmVsbGFAcGVjLml0-9v5lpl-p0auhh-0anbzk/MDE3MDAwNTM0NzY=

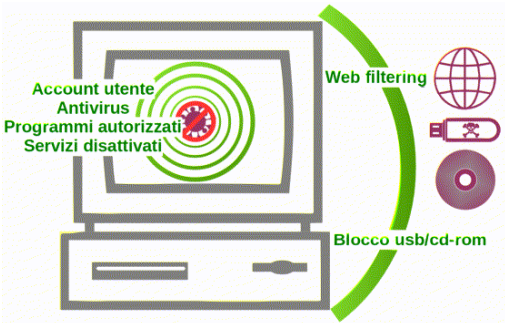
Gli effetti di un ransomware

Il malware di tipo ransomware è un programma che una volta attivatosi cripta tutti i file contenuti nel computer propagandosi anche a tutti gli apparati connessi.
A questo punto tutti i file non sono più leggibili e solitamente viene richiesto un riscatto per avere il codice di sblocco.
Al momento nemmeno le società produttrici di antivirus riescono a sbloccare i file criptati da tutti i tipi di ransomware e non è sicuro che una volta pagato il riscatto si ottenga in risposta la soluzione.

Proteggere il computer

Si rende pertanto necessario approntare alcune misure preventive per prevenire e comunque ridurre i danni prodotti dal malware.
Ogni misura di sicurezza attivata lavora in sinergia con le altre creando strati di protezione che rendono ardua la possibilità che un malware possa entrare nel computer o comunque agire con effetti disastrosi.

- Doppio account: Amministratore e Utente
- Antivirus
- Abilitazione dei soli programmi autorizzati
- Disattivazione dei servizi non necessari
- Web filtering, accesso ad internet controllato
- Screensaver con blocco di accesso
- Blocco utilizzo porte usb/cd-rom
- Blocco bios dell'avvio da periferiche usb/cd-rom/rete



Programmi Open source

L'uso di software open source migliora la protezione in quanto presentano alcune caratteristiche peculiari rispetto i programmi commerciali.
La scelta di un programma soggiace a valutazioni tecniche e personali.
Premesso che un programma deve anzitutto soddisfare le esigenze dell'utilizzatore andrebbero valutate le seguenti caratteristiche:

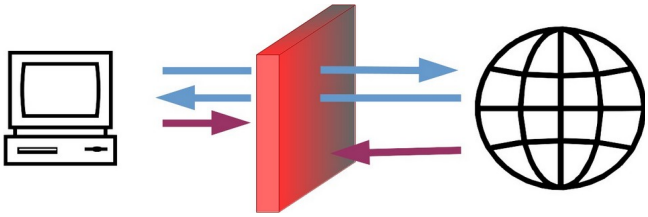
- **Multipiattaforma**, un programma compilato per i principali sistemi operativi Windows, Linux, Apple consente all'utente di passare da un OS all'altro potendo utilizzare lo stesso programma.
- **Open source**, un codice aperto potenzialmente ispezionabile avendone le adeguate conoscenze garantisce che il programma non contiene codice indesiderato. I programmi commerciali sono 'chiusi' e per alcune normative è persino reato l'hacking degli stessi – essendo soggetti ad un restrittivo copyright – impedendo di fatto di valutare un eventuale comportamento illecito o penalizzante per la privacy.
- **Free/freeware**, questo tipo di licenza consente l'utilizzo libero del programma senza costi aggiuntivi. Alcuni programmi possono essere utilizzati liberamente ma solo per scopi NON commerciali.
- **Versione portable**, che non altera le impostazioni del sistema operativo. Molti programmi sono estremamente invasivi e modificano l'ambiente per adattarlo alle proprie esigenze. L'installazione di molti programmi potrebbe generare conflitti e rallentamenti del sistema operativo. Spesso la rimozione non è efficacie e lascia tracce della precedente installazione.
- **Possibili macro* dannose** annidate in un file e scritte specificatamente per programmi a larga diffusione non funzionano o comunque hanno minore efficacia su programmi alternativi.
  **piccoli programmi*

LibreOffice Firefox Thunderbird

Le pagine web sono piene di tracker JavaScript* che raccolgono le abitudini di navigazione dell'utente e i comportamenti,
oltre che di spazi pubblicitari che rallentano il caricamento delle pagine.
Per bloccarli è possibile installare dei plugin del programma di browsing internet.
**codice invisibile annidato nella pagina web*

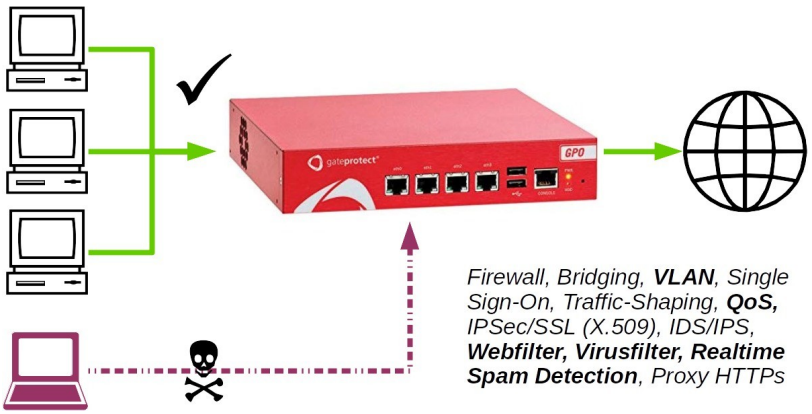
Firefox + GHOSTERY + uBlock Origin = PUB

Il Firewall



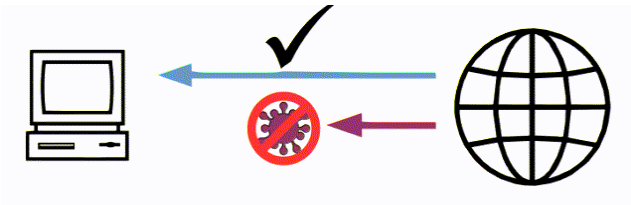
Il Firewall è un software che difende la rete interna (azienda, casa) dagli attacchi che provengono da quella esterna (internet) controllando tutto il traffico in entrata e in uscita.
Il firewall è un componente vitale di una strategia di sicurezza informatica ma la sua efficacia è legata alle regole con cui è stato configurato e quindi ad un compromesso tra usabilità e restrizioni.
Un parte importante delle minacce alla sicurezza informatica proviene dalla rete interna: portatili, connessioni abusive, accessi VPN, reti wireless non adeguatamente protette, attività inconsapevoli.

Il firewall può risiedere nel sistema operativo del computer o meglio ancora in un appliance* posto tra le rete aziendale e il collegamento ad internet. In questo modo ogni regola impostata avrà un immediato effetto di protezione su tutti gli apparati posti dietro il firewall.
Un firewall può essere configurato per riconoscere i computer che hanno accesso alla rete ed impedire connessioni abusive.
Ogni componente della rete può essere individuato tramite il suo ip (es. 192.168.1.89) o ancor meglio tramite il mac address (es. 00-08-74-4C-7F-1D).
**un dispositivo hardware progettato per un applicativo specifico*



*Firewall, Bridging, **VLAN**, Single Sign-On, Traffic-Shaping, **QoS,** IPSec/SSL (X.509), IDS/IPS, **Webfilter, Virusfilter, Realtime Spam Detection**, Proxy HTTPs*

Web filtering

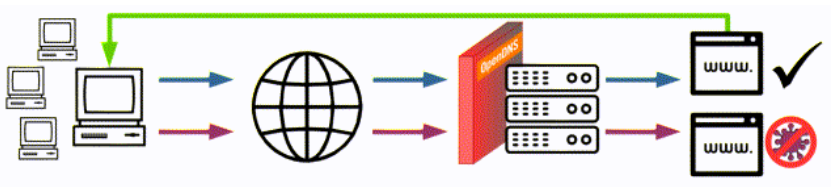


Sono quei software che raggruppano i siti web in categorie e impediscono l'accesso a quelli bloccati.
Poiché alcuni siti web devono poter essere raggiunti per motivi di lavoro, è possibile attivare una "white list" di pagine web autorizzate.
Il processo richiede del tempo per identificare tutte le pagine web da autorizzare.

OpenDns – Cisco Umbrella offre un servizio cloud* di sicurezza (free uso home) che protegge contro malware, phishing e callback di comando e controllo.

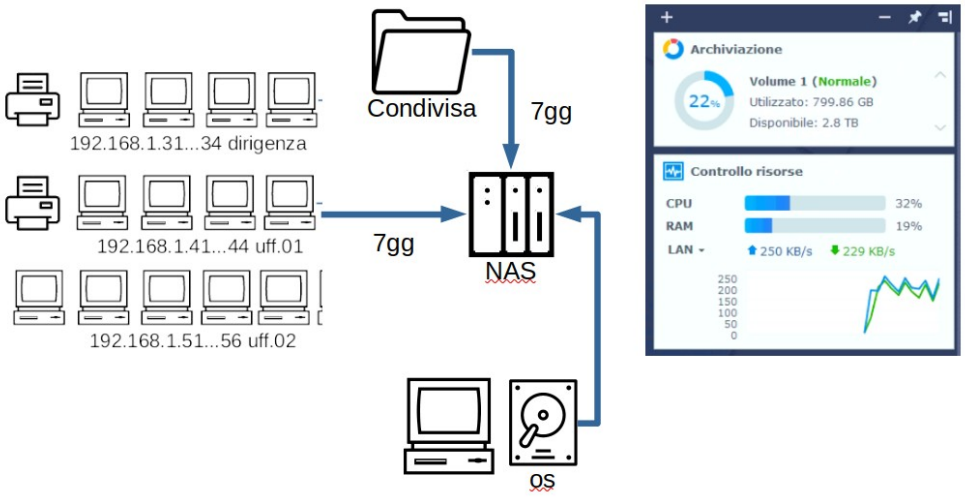
- consente un solo gruppo di regole per l'IP di partenza.
- permette l'impostazione di white list e black list.

** l'utilizzo di risorse hardware o software da remoto*



Backup dati

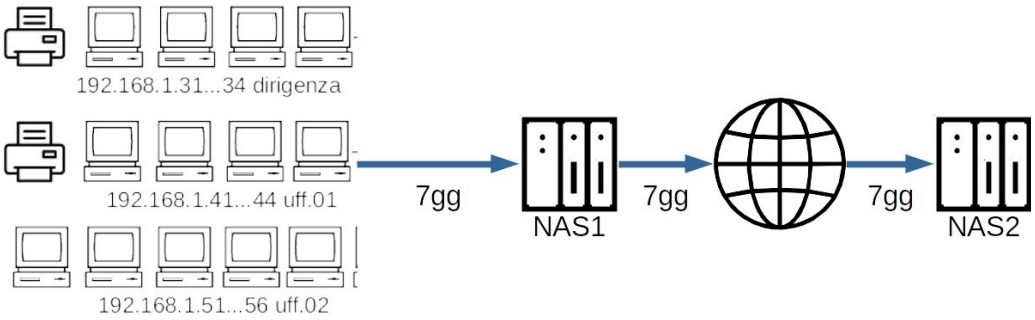
La copia dei dati su dispositivi di archiviazione esterni è la miglior strategia di sicurezza.



Solitamente si utilizza un nas (Network Attached Storage) ovvero un dispositivo composto da uno o più harddisk e collegato alla rete, che consente l'accesso alle informazioni in lettura/scrittura a più utenti secondo determinate regole.
Le copie vanno effettuate ad intervalli regolari e mantenute per un periodo di tempo adeguato in modo da poter recuperare i dati anche a distanza di giorni.
Prendiamo il caso di un backup giornaliero che viene sovrascritto ogni volta. Se a distanza qualche giornio ci rendiamo conto che un documento è stato modificato in modo errato, non avremo la possibilità di recuperare una vecchia copia. Potremo farlo se il backup mantiene le copie vecchie per un periodo di tempo sufficientemente lungo.
Il numero di backup mantenuti dipende dalla quantità di dati da proteggere e dalle dimensioni degli harddisk del nas; solitamente si consiglia di mantenere le vecchie copie per almeno 7gg ma laddove sia necessario si possono prevedere periodi più lunghi, o addirittura predisporre backup a scadenze orarie.

Ridondanza dei backup

Come visto in precedenza anche il nas potrebbe essere oggetto di attacco malware con conseguente perdita di tutti i dati contenuti.
Pertanto sarebbe ottimale eseguire un "backup del backup" su altro dispositivo nas disconnesso dalla rete se non durante la fase di copia.



Ottimizzare il computer

Di seguito le impostazioni consigliate per un computer ad uso aziendale presupponendo che il OS sia Windows 7/8/10.

livello di importanza	*operazioni da effettuare*

alto	• doppio utente:
	  • admin-xx pwd: XXxxnnnn$ con privilegi admin; questo utente NON va usato se non per operazioni di amministrazione sistema, es. installazione programmi/periferiche.
	  • utente-xx pwd: XXxxnnnn$ con privilegi standard; questo è l'utente da utilizzare per le normali operazioni di lavoro giornaliero.
	• installare antivirus ; suggeriamo Panda nella versione free. L'antivirus si aggiorna automaticamente.
	• installare programma di blocco dei programmi non autorizzati ; suggeriamo RunBlock.
	• installare un programma di backup dati ; suggeriamo EVAcopy-backup.
	  • impostare il programma in modo che ad intervalli regolari esegua automaticamente le copie su una unità di memoria esterna usb/nas.
	  l'unità di backup deve essere protetta e non deve risiedere in prossimità del computer.
	• ripartizione hard disk in C: e D:
	  • partizione C: Win10 dove risiede il sistema operativo.
	  • partizione D: Doc dove risiedono i dati dell'utente ed eventuali nuovi programmi installati.
	  • disattivazione indicizzazione hard disk C: e D: per velocizzare l'accesso ai dati.
	• aggiornamenti del OS.
	• rinomina del pc in xx-pc31.
	• assegnazione di un ip di rete intranet statico es. 192.168.1.31 ; tale procedura va eseguita per tutti gli apparati della rete secondo uno schema codificato.
	• disattivare la connessione al desktop remoto.
	• impostazioni di privacy per ridurre l'invio di dati non autorizzati ; alcuni programmi di Microsoft (es. Skype) potrebbero non funzionare.
	• disattivazione delle app in background.

medio	• impostare lo swap fisso a nGB dipendentemente dalla ram disponibile.
	• rimozione programmi non necessari:
	xbox, cortana, winrar, visualizzatore 3d, giochi, amazon, 3d builder, hub di feedback, il tuo telefono, piani dati mobili, paint 3d, MS pay, one drive, print 3d, brand bloatware, driver non più in uso
	• pulizia utilità di pianificazione.
	• pulizia del registro di sistema
	• installazione ZiS-Suite programmi portable.
	  • Firefox browser internet.
	  • Thunderbird browser di posta.
	  • Libreoffice suite di office automation (documenti, fogli di calcolo, presentazioni, disegno).
	  • Vlc lettore multimediale audio e video.
	  • Pdf-Xchange visualizzatore ed editore di file pdf.
	• associazione delle estensioni file con relativi programmi portable.
	• spostamento cartelle utente su partizione D:

basso	• impostazione grafica del desktop per un razionale uso aziendale. • riduzione degli effetti visivi al minimo. • configurazione del menu/start. • attivare screensaver 15 minuti con password all'accesso come da normativa vigente. • disattivare sospensione computer.
alto	• deframmentazione hard disk a doppio passaggio (solo per hhd, no ssd). • immagine di backup del OS per un eventuale ripristino ; suggeriamo l'utlity di Windows + Clonezilla
Interventi possibili per migliorare le prestazioni del computer	• espandere la ram per evitare l'uso dello swap file ; si raccomanda di far eseguire l'upgrade presso un centro specializzato che individui il tipo corretto di RAM da aggiungere/sostituire. • installare una unità ups (batteria tampone) per prevenire sbalzi/ammanchi di tensione. • sostituire l'attuale disco fisso meccanico (hhd) con uno a stato solido (ssd).
Operazioni da eseguire regolarmente	• riavviare il computer giornalmente. • deframmentare regolarmente l'hard disk (solo per hhd, no ssd).