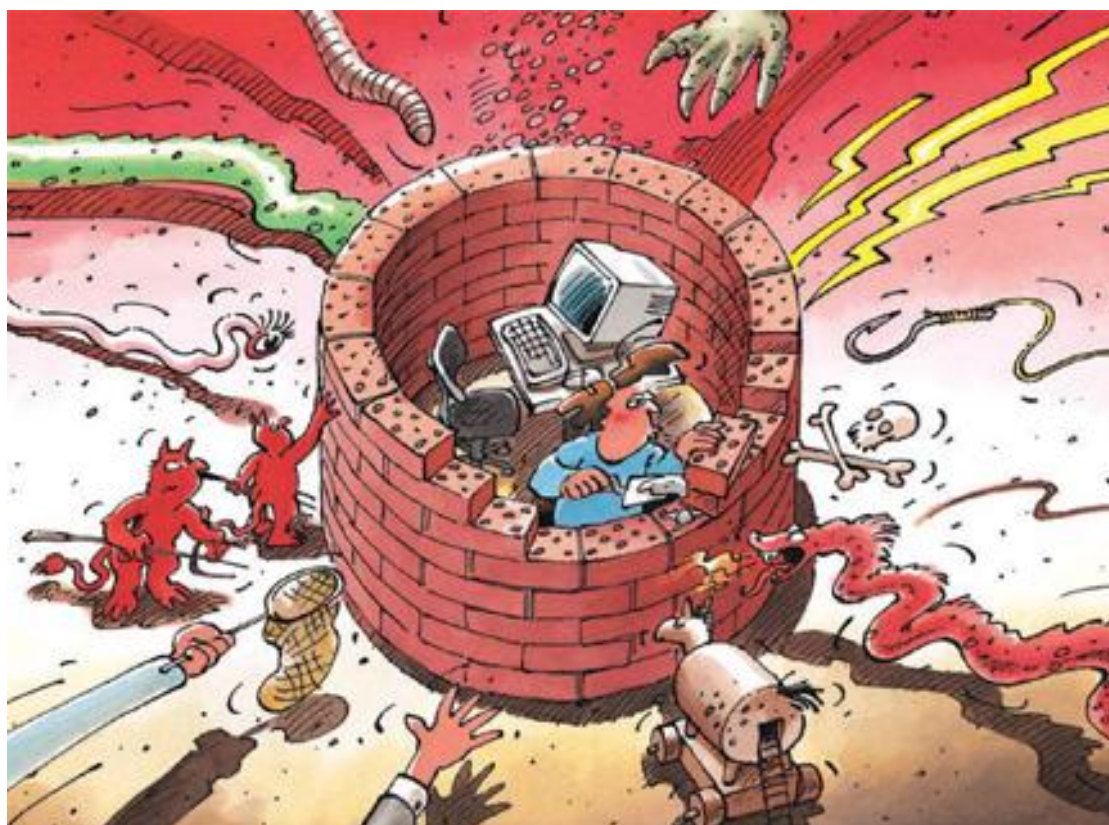


Parametri di sicurezza per Windows XP

Documento disponibile all'indirizzo: www.melani.admin.ch



Versione 1.1
15.07.2005

Lista di controllo «Parametri di sicurezza per Windows XP»

I singoli punti sono spiegati passo per passo nelle pagine successive.

Personal firewall

Verificate regolarmente se il firewall disponibile in Windows XP è attivato e non ammettete nessuna eccezione. Questa funzione può essere controllata e attivata nel centro di sicurezza (*Pannello di controllo → Centro sicurezza PC → Windows Firewall*).

Aggiornamenti del software

Attivate la funzione di aggiornamento automatico, il cui menu di configurazione è parimenti accessibile tramite il centro di sicurezza (*Pannello di controllo → Centro sicurezza PC → Aggiornamenti automatici*).

Non scordate di attualizzare regolarmente anche gli altri software (ad es. MS Office, Audio Player ecc.).

Software antivirus

Sinceratevi dell'installazione di un software antivirus e mantenetelo aggiornato per il tramite della funzione di aggiornamento automatico.

Gestione dei conti di utente

Assegnate una potente password a ogni conto di utente.

Salvaguardia dei dati

Effettuate regolarmente la salvaguardia dei dati su un supporto esterno di dati e verificate di tanto in tanto se i dati possono essere ripristinati.

Conservate i supporti esterni di dati in un luogo sicuro.

INDICE

<u>INTRODUZIONE</u>	1
<u>PROTEZIONE DI BASE</u>	2
PERSONAL FIREWALL	2
AGGIORNAMENTI DEL SOFTWARE	3
SOFTWARE ANTIVIRUS (PROTEZIONE CONTRO IL MALICIOUS CODE)	4
OPZIONI DI INTERNET	5
GESTIONE DEI CONTI DI UTENTE	7
WINDOWS XP HOME	7
WINDOWS XP PROFESSIONAL	9
SALVAGUARDIA DEI DATI	11
<u>PARAMETRI COMPLEMENTARI DI SICUREZZA</u>	12
OPZIONI DI LOGIN	12
PARAMETRI LOCALI DI SICUREZZA SOTTO WINDOWS XP PROFESSIONAL	13
CRITERI PER LA PASSWORD	13
CRITERI DI BLOCCO DEL CONTO	15
CRITERI DI CONTROLLO	16
ASSEGNAZIONE DI DIRITTI DI UTENTE	16
OPZIONI DI PROTEZIONE	17
SERVIZI	17
CONTROLLO E LIMITAZIONE DEI COLLEGAMENTI USCENTI	17
CRITTOGRAFIA DEI DATI SOTTO WINDOWS XP PROFESSIONAL	18
DISATTIVAZIONE DELLA CONDIVISIONE DI FILE E STAMPANTI	18
BLOCCO DEL DESKTOP E SALVASCHERMO	21
<u>VERIFICA DELLA SICUREZZA DI SISTEMA PER IL TRAMITE DI TOOLS</u>	21
MICROSOFT BASELINE SECURITY ANALYZER (MBSA)	21
REPERIMENTO E RIMOZIONE DI SPYWARE E DI ADWARE	21
<u>RIFERIMENTI E LINK SU INFORMAZIONI COMPLEMENTARI</u>	23
<u>ALLEGATO A: DETERMINAZIONE DEL SERVICE PACK INSTALLATO</u>	24
<u>ALLEGATO B: VISUALIZZAZIONE DELLE INFORMAZIONI SUL FILESYSTEM</u>	24

Introduzione

Osservando poche misure e norme di comportamento il vostro sistema Windows XP è già ben protetto contro gli accessi non autorizzati e le ripercussioni di virus, vermi informatici e cavalli di Troia. Tali misure comprendono

- il personal firewall
- gli aggiornamenti del software
- il software antivirus
- la salvaguardia dei dati

e sono descritte nel primo capitolo «Protezione di base». Il capitolo immediatamente successivo, «Parametri complementari di sicurezza», si rivolge agli utenti esperti di Windows. Le raccomandazioni ivi contenute contribuiscono a potenziare la sicurezza al di là della protezione di base.

Avvisi importanti:

- Windows XP esiste in una Home Edition e in una Professional Edition. Le due versioni si differenziano su taluni punti. La presente guida tiene conto nella misura del possibile di questa circostanza.
- Il presente documento è valido unicamente per i sistemi Windows XP che non fanno parte di un dominio Windows. Ne è sempre il caso trattandosi di utenti privati.
- Si suppone inoltre che il sistema Windows XP corrisponda all'ultimo stato di aggiornamento in fatto di service pack (attualmente SP2) e di aggiornamenti di sicurezza¹ e che il filesystem sia NTFS².

¹ L'«Allegato A: Determinazione del service pack installato» indica come verificare questo parametro.

² L'«Allegato B: Visualizzazione delle informazioni sul filesystem» indica come verificare questo parametro.

Protezione di base

Windows XP è attualmente il sistema operativo cliente più attuale di Microsoft. Nell'ambito del service pack 2 (SP2) vi è stato aggiunto il centro di sicurezza, comprensivo dei tre punti centrali *firewall*, *aggiornamenti automatici* e *protezione da virus*. L'interfaccia utente è accessibile tramite la rubrica di menu «Pannello di controllo → Centro sicurezza PC».



Illustrazione 1: il centro di sicurezza di Windows

Le pagine che seguono abordano alcuni aspetti del centro di sicurezza e delle sue funzioni.

Personal firewall

Un firewall protegge i sistemi di computer, nel senso che sorveglia i collegamenti entranti e uscenti e se del caso li rifiuta. La decisione di accettazione o di rifiuto dei collegamenti poggia su regole semplici, oggetto di verifica ad ogni nuovo collegamento.

L'installazione del service pack 2 attiva in modo standard il firewall integrato in Windows XP. Il menu di configurazione del firewall di Windows è accessibile per il tramite del centro di sicurezza (cfr. illustrazione 1). I parametri desiderati possono essere selezionati intervenendo sulle tre schede «Generale», «Eccezioni» e «Avanzate» (cfr. illustrazione 2).

- Verificate nella scheda «Generale» se è stato selezionato il pulsante «Attivato» sulla finestra dell'illustrazione 2 e contrassegnate il campo «Non consentire eccezioni».

Gli utenti esperti possono liberare l'accesso ai servizi della scheda «*Eccezioni*», se utilizzano ad esempio servizi come la condivisione dei dati e delle stampanti.

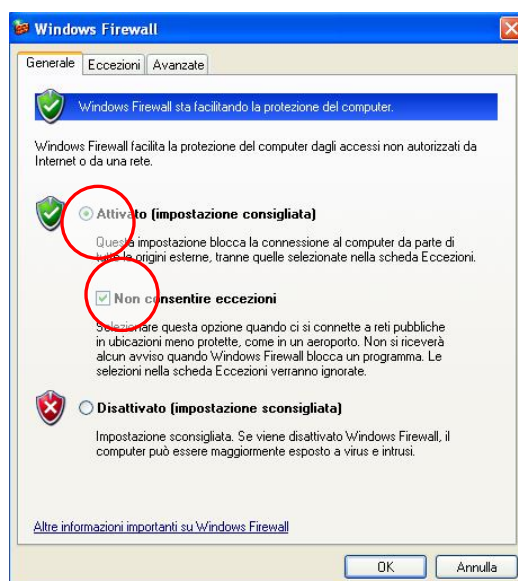


Illustrazione 2: configurazione del firewall di Windows

Avviso importante: il firewall di Windows consente unicamente il controllo dei collegamenti entranti. Non è possibile controllare e sorvegliare i collegamenti in uscita dal sistema! Ulteriori informazioni in merito sono disponibili nella sezione «Controllo e limitazione dei collegamenti uscenti» a [pagina 17](#).

Aggiornamenti del software

Le lacune di sicurezza possono rendere possibile l'accesso non autorizzato ai dati o la diffusione di vermi informatici e possono verificarsi sia a livello di sistemi operativi (ad es. Windows XP, Windows 2000, Mac OS X, Linux ecc.), sia a livello di applicazioni (ad es. Internet Explorer, Media Player ecc.). Per accrescere la sicurezza dei vostri dati (e degli altri utenti di Internet) assume pertanto grande importanza l'installazione regolare di aggiornamenti di sicurezza, che colmano queste lacune di sicurezza.

La funzione di aggiornamento automatico di Windows XP è parimenti accessibile tramite il centro di sicurezza e deve essere assolutamente attivata (cfr. illustrazione 3). Ricordatevi che la funzione di aggiornamento concerne unicamente il sistema operativo, Internet Explorer, Media Player ecc., ma non MS Office (Word, Excel, PowerPoint, Access, Outlook). Questi ultimi aggiornamenti devono essere effettuati separatamente tramite la pagina Web di Microsoft, che dovrete consultare regolarmente a tale scopo:

<http://office.microsoft.com/it-it/officeupdate/default.aspx>

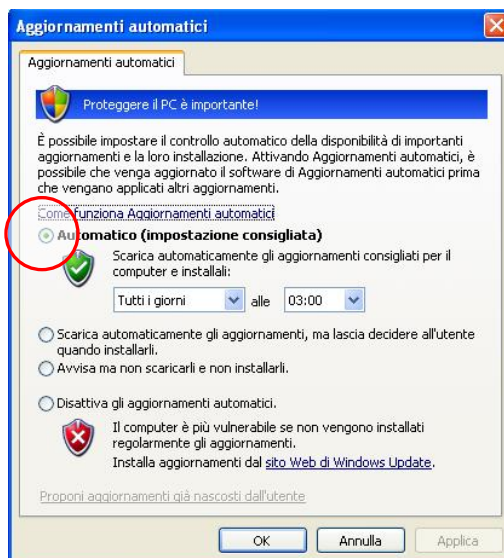


Illustrazione 3: aggiornamento automatico del software

Oltre al sistema operativo e alle applicazioni di Office, devono essere periodicamente verificati quanto alla loro attualità i prodotti software di offerenti terzi (ad es. software di spaccettaggio, reader di documenti). Nel caso dei programmi che non dispongono di una funzione di aggiornamento automatico si raccomanda di consultare regolarmente le pagine Web dei pertinenti produttori.

Software antivirus (protezione contro il malicious code)

Malicious code è il termine generico per software che esegue funzioni nocive su un computer. Oltre ai virus, rientrano tra l'altro in questo gruppo i vermi informatici e i cavalli di Troia. Informazioni dettagliate in merito a questi concetti si trovano al seguente link della pagina Web di MELANI:

<http://www.melani.admin.ch/gefahren-schutz/schutz/index.html?lang=it>

Provvedete assolutamente affinché un software antivirus aggiornato sia disponibile sul vostro sistema. Il software antivirus non protegge unicamente i dati sul vostro sistema, ma anche i sistemi e i dati degli altri utenti di Internet. A titolo di esempio, l'invio di spam si avvale di sistemi insufficientemente protetti, senza che l'utente se ne accorga. Anche simili pericoli possono essere ridotti a un minimo grazie a una protezione antivirus aggiornata.

Windows XP cerca di identificare il software antivirus installato e di verificarne lo stato di aggiornamento. Se il tentativo di identificazione fallisce o se il software antivirus non è aggiornato oppure non è disponibile, ne è dato avviso all'utente per il tramite di un'icona nella barra delle applicazioni e di un'evidenziazione in rosso della rubrica di menu «Protezione da virus» del centro di sicurezza (illustrazione 4).



Illustrazione 4: rilevamento dell'assenza di protezione antivirus (evidenziato in rosso)

In questo caso procuratevi immediatamente un software antivirus e mantenetelo aggiornato per il tramite della funzione di aggiornamento automatico. Il seguente link vi fornisce una selezione di simili programmi di protezione:

http://www.melani.admin.ch/gefahren-schutz/links/index.html?lang=it#sprungmarke2_4

Opzioni di Internet

Anche le opzioni di Internet sono accessibili per il tramite del centro di sicurezza di Windows (cfr. illustrazione 4, in basso a sinistra). Selezionate la scheda «Protezione» (cfr. illustrazione 5, a sinistra):

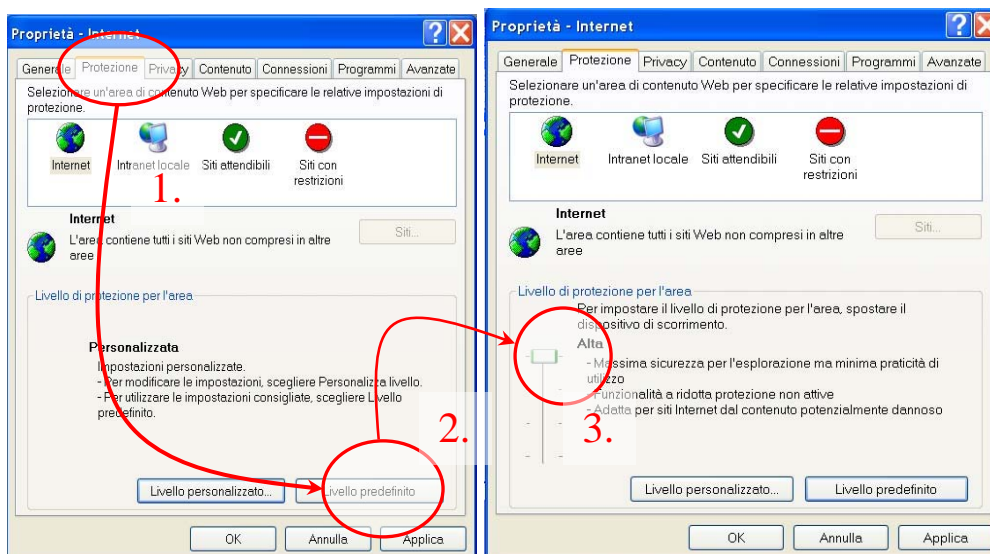


Illustrazione 5: scheda «Protezione»

Selezionate per l'area «Internet» il livello di protezione predefinito «Alta». A tale scopo basta agire sul dispositivo di scorrimento del pulsante «Livello predefinito».

Selezionate successivamente per l'area «*Siti attendibili*» il livello predefinito «*Bassa*» e cliccate sul pulsante «*Siti...*». Si apre allora una finestra come quella dell'illustrazione 6.

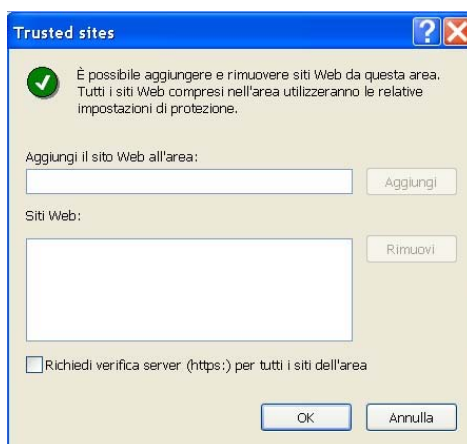


Illustrazione 6: Definizione di pagine Web attendibili

Eliminate il contrassegno dall'opzione «*Richiedi verifica server (https:) per tutti i siti dell'area*». Inserite qui la homepage della vostra banca online (ad es. <https://vostrabancaonline.ch>) e la homepage di Windows Update (*.update.microsoft.com , *.windowsupdate.microsoft.com e *.windowsupdate.com). Aggiungete per prima cosa l'indirizzo nel campo superiore e cliccate successivamente sul pulsante «*Aggiungi*». Verificate l'esatta ortografia. Se la trasmissione viene effettuata per il tramite di un collegamento sicuro, all'indirizzo deve essere anteposto in modo corrispondente <https://>. Il segno * può essere utilizzato come segnaposto.

Avviso: se dopo aver selezionato questi parametri alcune homepage non dovessero più essere visualizzate correttamente, è possibile porvi rimedio riducendo a «*Media*» il livello predefinito di protezione dell'area «*Internet*». Non scordate di ripristinare il livello di protezione «*Alta*» al termine della visita delle singole homepage.

Gestione dei conti di utente

Windows XP Home

Durante l'installazione di Windows XP Home deve essere creato un conto di utente. Questo conto e tutti gli altri conti di utente creati successivamente dispongono per default di diritti di amministratore e non sono protetti da una password! Si tratta di un rischio per la sicurezza da eliminare immediatamente. Avviate la gestione degli utenti selezionando «*Pannello di controllo* → *Account utente*»; appare allora la finestra dell'illustrazione 7:

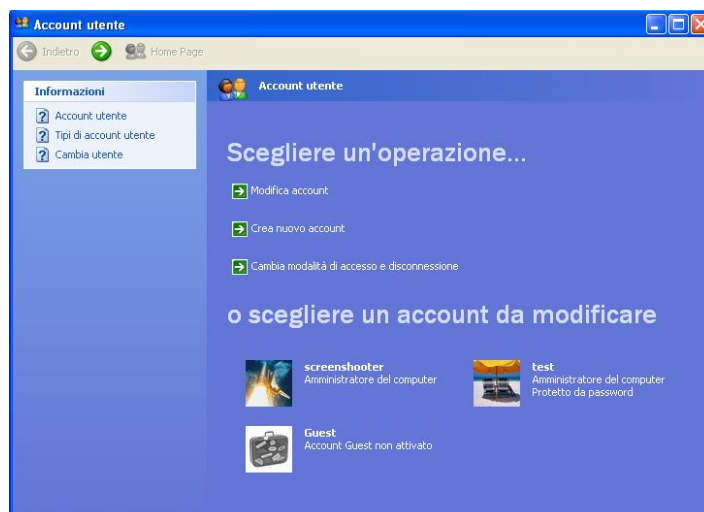


Illustrazione 7: utenti definiti

- Verificate anzitutto se il conto guest è disattivato. Se del caso disattivatelo.
- Definite successivamente una password per ogni conto di utente, cliccando sul conto corrispondente, che apre la finestra di cui all'illustrazione 8.
- Cliccate su «*Cambiare password*» (cfr. illustrazione 9).



Illustrazione 8: proprietà del conto di utente «test»

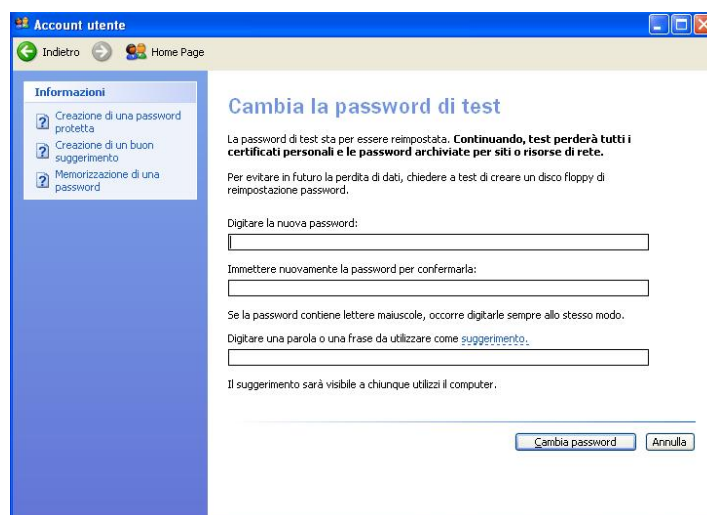


Illustrazione 9: definizione di una password per il conto di utente «test»

Visto che per default non viene definita alcuna password, il primo campo può essere lasciato vuoto. Assegnate a ogni conto di utente una password difficilmente rintracciabile ed evitate di annotarla. Nella scelta della password osservate i seguenti principi:

- le password devono constare di lettere dell'alfabeto, di cifre e di caratteri speciali
- la lunghezza minima non deve essere al di sotto di 8 caratteri
- le password devono essere modificate regolarmente (ogni 3 mesi circa)

Utilizzate suggerimenti mnemonici per la scelta della password. Ecco un esempio:

Termine iniziale:	ciaociao
Maiuscole /minuscole:	CiaoCiao
Inserimento di cifre:	C1a0C1a0
Inserimento di caratteri speciali:	C1@0C1@0

Utilizzate di volta in volta password diverse per scopi diversi (ad. es. per l'e-banking, il vostro computer, altri servizi online).

Oltre ai conti di utente che avete creato, sul sistema si trova un ulteriore conto (amministratore) con diritti di amministratore, che non appare nella visualizzazione «Account utente» (illustrazione 7). Per poter modificare la password di questo utente dovete eseguire nel menu d'avvio «Esegui...» il comando «*control userpasswords2*». È visualizzata in questo caso la finestra dell'illustrazione 10. Attivando il pulsante «*Reimposta password*» è possibile definire una nuova password per il conto di utente nascosto.

Attenzione: non dovete in nessun caso scordare questa password. Altrimenti in caso di perdita delle password dei conti che avete creato, non vi sarà possibile reimpostare queste password.



Illustrazione 10: definizione della password del conto nascosto di amministratore

Windows XP Professional

La gestione degli utenti sotto Windows XP Professional è analoga. L'assegnazione di una password per il conto «nascosto» di amministratore viene però richiesta al momento dell'installazione.

- La definizione delle password per i conti che avete creato è effettuata in modo analogo a Windows XP Home.
- Per i conti di utente non visibili l'assegnazione può essere effettuata in modo analogo a Windows XP Home per il tramite del comando «*control userpasswords2*». Nondimeno tale definizione è più semplice per il tramite del «*Pannello di controllo*» (cfr. illustrazione 11).

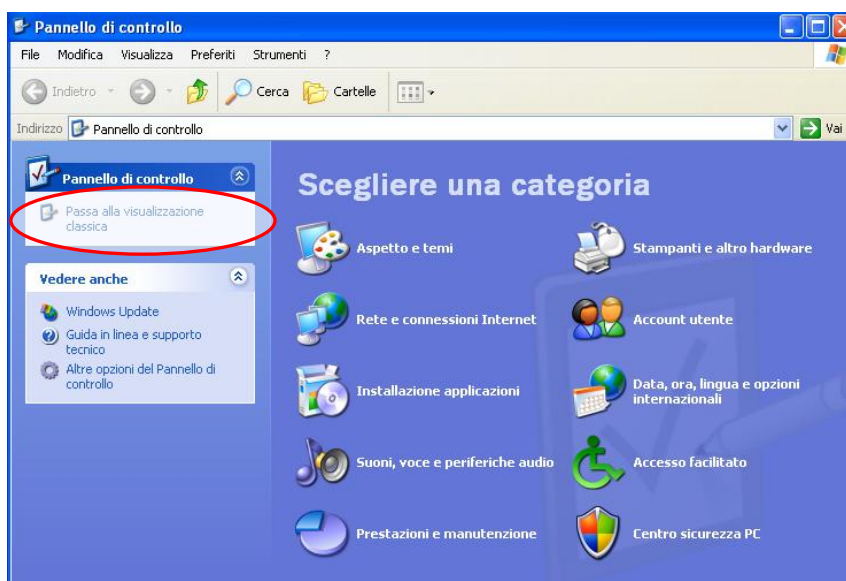


Illustrazione 11: pannello di controllo con selezione limitata

Passate alla visualizzazione classica cliccando sul campo corrispondente in alto a sinistra (posizione segnalata in rosso nell'illustrazione 11). La presentazione e il numero delle singole categorie ne vengono modificate (cfr. illustrazione 12).

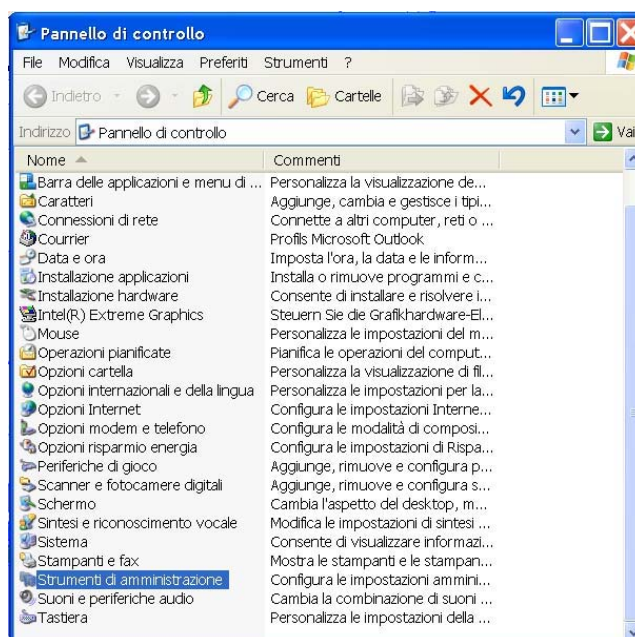


Illustrazione 12: visualizzazione classica del pannello di controllo

Per il tramite della rubrica di menu «*Pannello di controllo* → *Strumenti di amministrazione* → *Gestione del computer (Computer Management)* → *Utenti e gruppi locali* → *Users*» è possibile visualizzare i conti di utente esistenti. Per definire una password, selezionate il nome di utente desiderato e cliccate sul tasto destro del mouse. Successivamente definite la password.

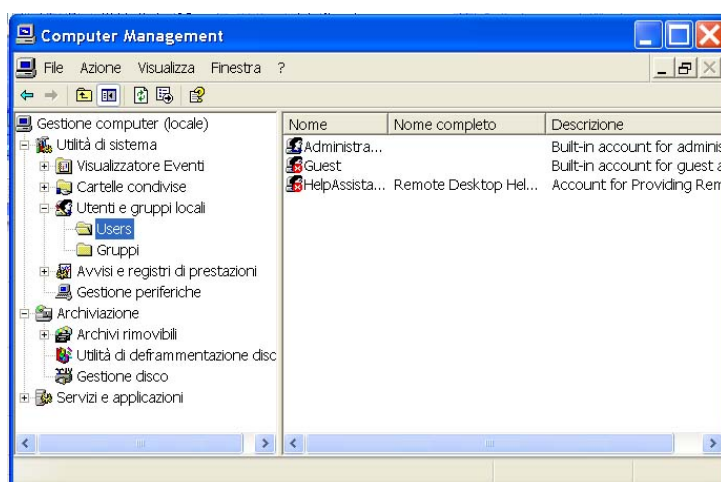


Illustrazione 13: visualizzazione di tutti i conti di utente sotto Windows XP Professional

Salvaguardia dei dati

Nonostante tutte le misure cautelari, i dati possono essere irrimediabilmente persi. La perdita dei dati non è imperativamente dovuta a un virus o a un attacco, ma può ad esempio risultare da un difetto tecnico. Per questo motivo si raccomanda di effettuare regolarmente la salvaguardia dei dati (backup). In questo contesto va osservato che i backup devono essere regolarmente controllati quanto alla loro capacità di ripristino (ossia leggibilità e integralità).

I dati salvaguardati devono essere copiati su un supporto esterno di dati, ad esempio un CD-ROM, un DVD o un disco rigido esterno, e conservati in un luogo protetto. Ulteriori informazioni sono disponibili al seguente indirizzo:

<http://www.melani.admin.ch/gefahren-schutz/schutz/00034/index.html?lang=it>

Parametri complementari di sicurezza

Osservando le raccomandazioni presentate nel capitolo precedente, viene raggiunta una solida protezione di base. È nondimeno possibile realizzare ulteriori miglioramenti nella sicurezza del sistema, che verranno trattati qui di seguito. Tali configurazioni dovranno soprattutto essere applicate se esistono più conti di utente sul sistema, se si può accedere al sistema dall'esterno o se è indispensabile un grado di protezione più elevato.

Avvisi importanti:

Le raccomandazioni illustrate qui di seguito devono essere attuate unicamente da utenti esperti di Windows. In precedenza i dati più importanti devono essere salvaguardati su un supporto esterno di dati.

MELANI non può assumere alcuna responsabilità per i danni insorti a causa di una configurazione errata del computer!

Opzioni di login

All'avvio di un sistema Windows XP è visualizzata una schermata di benvenuto (Welcome-Screen), contenente informazioni sui conti di utente esistenti. Tali informazioni possono fornire indicazioni non necessarie a persone non autorizzate e semplificare un accesso non autorizzato al sistema. Per evitare questi inconvenienti si dovrebbe utilizzare la schermata classica di login (schermata di login). È possibile accedervi alla rubrica «*Cambia modalità di accesso e disconnessione*» del menu «*Pannello di controllo* → *Account utente*», dove dovete rimuovere la crocetta da «*Usa la schermata iniziale*».

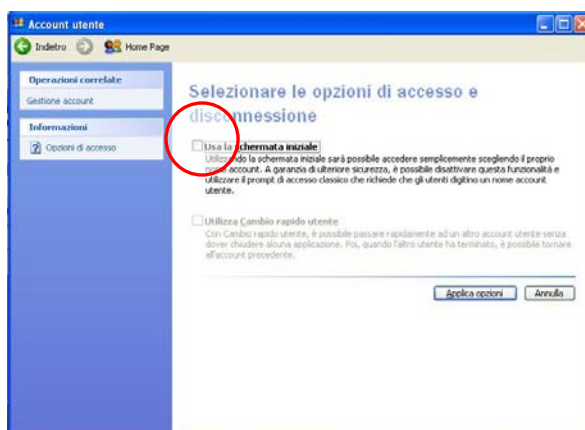


Illustrazione 14: attivazione della schermata classica di login

È predefinita la visualizzazione dell'ultimo utente che ha effettuato il login, ma anche questa visualizzazione può essere mascherata:

- **Windows XP Home:** digitate nel menu di avvio «Esegui...» il comando *regedt32*. Sotto «HKEY_LOCAL_MACHINE → SOFTWARE → Microsoft → Windows → CurrentVersion → policies → system» selezionate il valore 1 per «*dontdisplaylastusername*».
- **Windows XP Professional:** selezionate «Pannello di controllo → Criteri di protezione locali → Impostazioni protezione» e nella finestra di destra sotto il criterio «Logon interattivo: non mostrare il nome dell'ultimo utente» modificate il criterio di sicurezza in «Attivato».

Parametri locali di sicurezza sotto Windows XP Professional

Nel menu «Pannello di controllo → Strumenti di amministrazione → Criteri di protezione locali (Local Security Settings)» è possibile effettuare diverse configurazioni locali dal profilo della sicurezza. Si tratta in particolare dei *criteri di account*, dei *criteri di blocco account*, dei *criteri di controllo*, dell'*assegnazione dei diritti di utente*, nonché di ulteriori impostazioni sotto la rubrica *opzioni di protezione*. I criteri di account e di password possono essere configurati per il tramite delle rubriche di menu *criterio password* e *criterio di blocco account*. I parametri raccomandati sono elencati qui appresso.

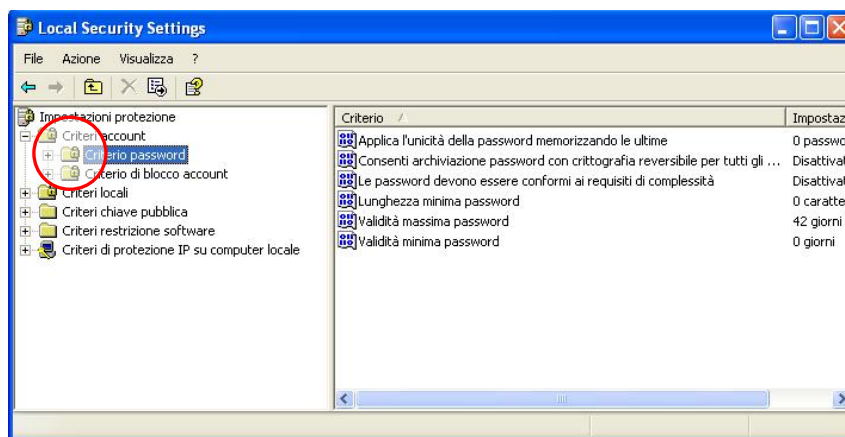


Illustrazione 15: configurazione dei criteri di account e di password

Criteri per la password

<i>Le password devono essere conformi ai criteri di complessità:</i>	Attivando questo parametro la password deve constare di lettere maiuscole e minuscole, di cifre e di caratteri speciali. Questa impostazione è però attivata soltanto all'atto della prossima modifica della password da parte dell'utente. Le password già definite ne sono escluse. <i>Impostazione raccomandata: Attivato</i>
<i>Applica l'unicità della</i>	Questa impostazione impedisce che l'utente possa

<p><i>password memorizzando le ultime:</i></p>	<p>definire password già utilizzate in caso di modifica coatta. Il parametro selezionato indica il numero di password memorizzate dal sistema. Se tale parametro corrisponde ad esempio a 12, l'utente può ripristinare la sua prima password all'atto della 13^a modifica. La fascia di valori è compresa tra 0 (l'utente può immediatamente riutilizzare la vecchia password) e 24.</p> <p><i>Impostazione raccomandata: 12</i></p>
<p><i>Consenti archiviazione password con crittografia reversibile per tutti gli utenti del dominio:</i></p>	<p><i>Impostazione raccomandata: Disattivato</i></p>
<p><i>Validità massima password:</i></p>	<p>Per questo tramite l'utente è obbligato a modificare la sua password a intervalli regolari.</p> <p><i>Impostazione raccomandata: 60 – 90 giorni</i></p>
<p><i>Validità minima password:</i></p>	<p>Anche questo parametro dovrebbe essere impostato per impedire che l'utente possa eludere l'impostazione «<i>Applica l'unicità della password memorizzando le ultime</i>». Nell'ipotesi contraria l'utente può modificare più volte in successione la password sino al ripristino di quella che gli è usuale.</p> <p><i>Impostazione raccomandata: 5 giorni</i></p>
<p><i>Lunghezza minima password:</i></p>	<p>Per i conti (account) che dispongono di speciali privilegi (ad es. amministratori) si raccomanda una lunghezza di 12 o più caratteri. Per gli utenti normali la lunghezza dovrebbe almeno essere impostata su 8 caratteri.</p> <p>Avviso: Windows XP supporta una lunghezza di password sino a 127 caratteri.</p>

Criteri di blocco del conto

Le impostazioni relative al blocco del conto devono essere operate nel secondo punto dei criteri account (cfr. illustrazione 16).

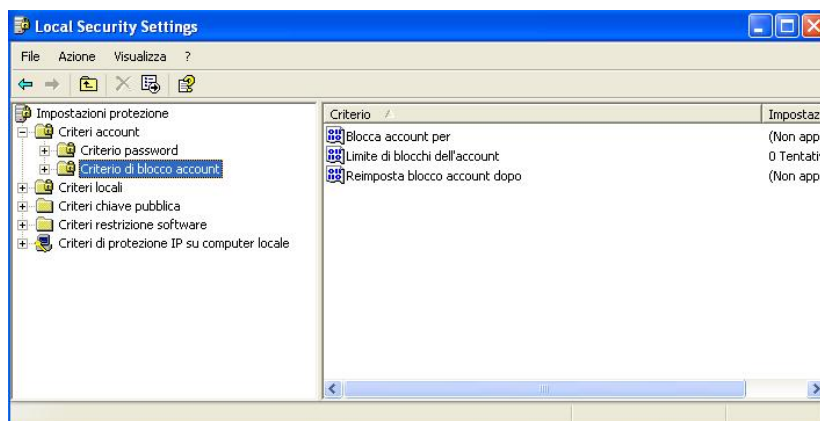


Illustrazione 16: blocco dei conti di utente

Si raccomandano le seguenti impostazioni:

<p><i>Limite di blocchi dell'account:</i></p>	<p>Viene qui definito il numero di tentativi non validi di login sino al blocco del conto. In tal modo si intendono impedire gli attacchi di brute-force per il tramite di strumenti automatizzati.</p> <p><i>Impostazione raccomandata:</i> 3 tentativi al massimo</p>
<p><i>Blocca account per:</i></p>	<p>Mediante questo parametro è possibile definire in minuti il blocco temporaneo del conto. La fascia di valori ammessi è compresa tra 0 e 99999 minuti.</p> <p><i>Avviso importante:</i> il valore 0 non significa affatto che il conto non viene bloccato, anzi è vero il contrario. In questo caso l'amministratore deve nuovamente liberare l'accesso al conto, il che può condurre a un attacco denial-of-service. A partire dal terminale si può sempre accedere al conto dell'amministratore e qui pertanto non è possibile alcun blocco.</p> <p><i>Impostazione raccomandata:</i> 15 – 30 minuti</p>

Reimposta blocco account dopo:	Imposta l'intervallo di tempo sino alla reimpostazione del valore del blocco del conto. <i>Impostazione raccomandata: 15 – 30 minuti</i>
---------------------------------------	---

Criteria di controllo

Questo menu consente di effettuare impostazioni concernenti eventi significativi ai fini della sicurezza, come le notifiche di sistema, la gestione dei conti, l'accesso ai dati, ecc. A seconda delle esigenze si impongono impostazioni differenziate adeguate. Le corrispondenti raccomandazioni possono essere consultate al seguente indirizzo:

<http://www.microsoft.com/italy/technet/security/guidance/secmod62.mspx#EIAA>

Assegnazione di diritti di utente

I diritti assegnati sono di massima impostati in modo adeguato.

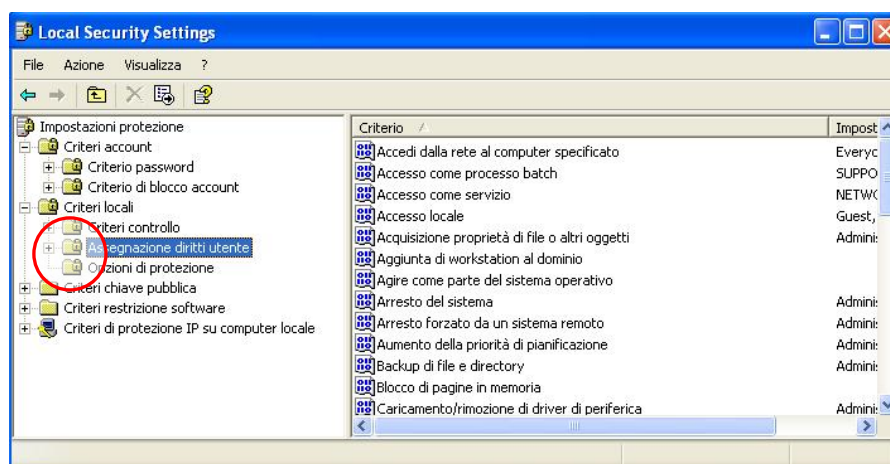


Illustrazione 17: impostazioni dei diritti di utente

Opzioni di protezione

Anche in questo caso le opzioni predefinite offrono già una buona sicurezza, pur consentendo adeguamenti individuali.



Illustrazione 18: opzioni di protezione

Servizi

Sui sistemi Windows XP installati in modo standard sono attivi servizi non necessariamente indispensabili all'uso quotidiano. A chi intende conoscere le finalità dei singoli servizi si raccomanda la consultazione del seguente link (in inglese):

http://www.theeldergeek.com/services_guide.htm

Il link contiene spiegazioni su ogni servizio, come pure raccomandazioni sul loro stato (attivato, manuale, disattivato). Gli adeguamenti dei servizi sono effettuati per il tramite del menu «Pannello di controllo → Strumenti di amministrazione → Servizi».

Controllo e limitazione dei collegamenti uscenti

Il firewall integrato di Windows non offre alcuna possibilità di controllo o di blocco dei collegamenti uscenti. Nell'ipotesi che giunga sul sistema, un malicious code può creare illimitatamente collegamenti verso l'esterno e così eventualmente trasmettere dati sensibili a un aggressore.

Si può ovviare a questo pericolo installando un personal firewall che possa altresì controllare e se del caso bloccare i collegamenti uscenti. Questo genere di prodotti è in parte disponibile gratuitamente su Internet.

http://www.melani.admin.ch/gefahren-schutz/links/index.html?lang=it#sprungmarke2_5

Crittografia dei dati sotto Windows XP Professional

Per garantire una protezione complementare dei dati sensibili, se ne raccomanda la crittografia per il tramite di EFS (Encrypting File System). Procedete come segue:

- Avviate Esplora risorse (Windows Explorer)
- Selezionate la directory da crittografare e aprite la corrispondente finestra delle proprietà (tasto destro del mouse → *Proprietà*)
- Cliccate sul pulsante «*Avanzate...*» della scheda «*Generale*»
- Contrassegnate il campo «*Crittografia contenuto per la protezione dei dati*» (cfr. illustrazione 19)
- Confermate la selezione cliccando sul pulsante «*OK*»

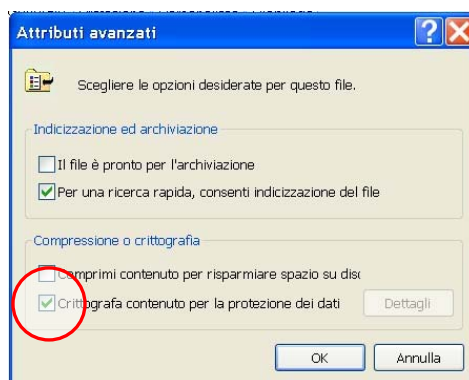


Illustrazione 19: crittografia dei dati

Benché i dati siano ora crittografati, non è visibile alcuna differenza perché Windows effettua automaticamente la decriptazione in background. Se però un altro utente tenta di accedere a questi dati, l'accesso gli è impedito con il messaggio di errore «*Accesso negato*».

Avviso importante: se più persone crittografano i dati per il tramite di EFS e a un determinato momento si rende necessaria una decriptazione coatta, al primo utilizzo di EFS deve esser implementato un cosiddetto recovery agent. Grazie ad esso è possibile decriptare tutti i dati in caso di emergenza. Guide sul tema sono consultabili ai seguenti indirizzi:

<http://support.microsoft.com/default.aspx?scid=kb:it:307877>
<http://www.fz-juelich.de/zam/files/docs/tki/tki-0397.pdf> (tedesco)

Attenzione: in caso di perdita della chiave di crittografia i dati cifrati con la stessa non sono più ripristinabili!!!

Disattivazione della condivisione di file e stampanti

Uno degli errori più frequenti in Windows è l'attivazione senza necessità della condivisione dei file e delle stampanti. Numerosi aggressori sfruttano questa funzione per accedere senza autorizzazione a singoli dati o all'intero sistema per il tramite di

entrambe le porte 139 e 445. Benché il firewall di Windows impedisca di massima l'accesso a questa funzione, se ne raccomanda la disattivazione a titolo di protezione complementare. La disattivazione viene operata accedendo alla rubrica di menu «Pannello di controllo → Connessioni di rete → Connessione LAN». Tramite il pulsante «Proprietà» viene attivata la finestra di destra dell'illustrazione 20. Disinstallate anzitutto entrambi i parametri «Client for Microsoft Networks» e «File and Printer Sharing for Microsoft Networks».

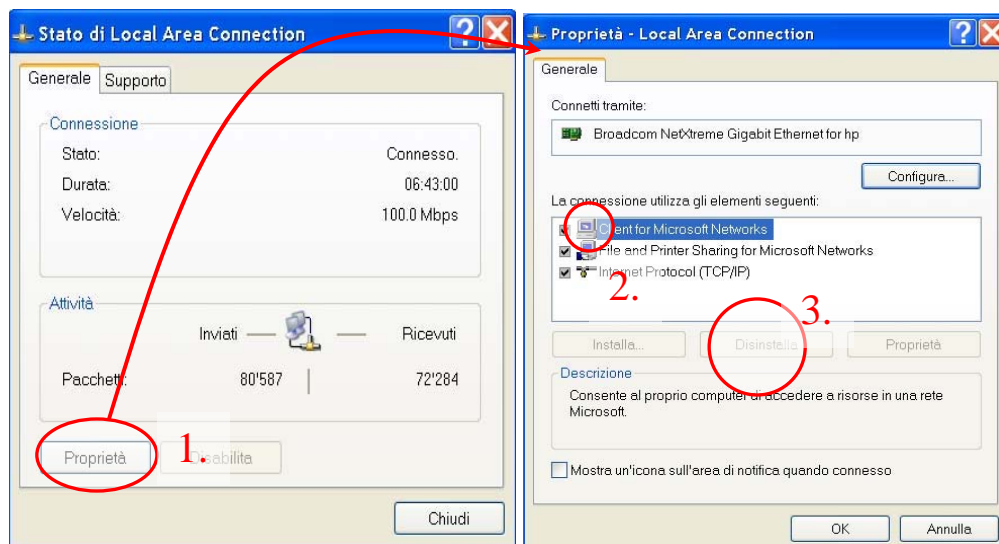


Illustrazione 20: proprietà del collegamento di rete

La finestra di destra dovrebbe successivamente corrispondere a quella dell'illustrazione 21.

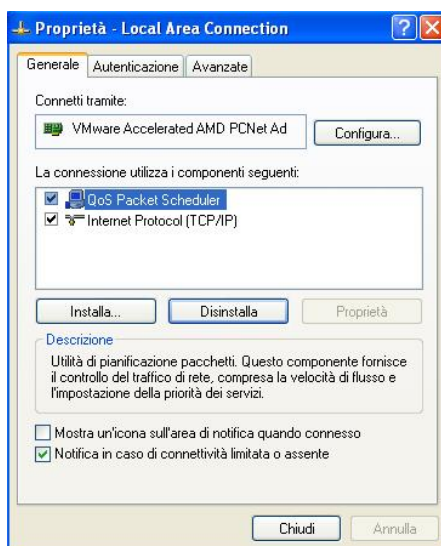


Illustrazione 21: stato dopo la disinstallazione di entrambi i servizi di rete

Cliccate due volte sulla rubrica «Internet Protocol (TCP/IP)» («Protocollo Internet (TCP/IP)») per fare apparire la finestra di sinistra dell'illustrazione 22. Cliccate

successivamente il pulsante «Avanzate...» e selezionate nella scheda WINS «Disabilita NetBIOS su TCP/IP».

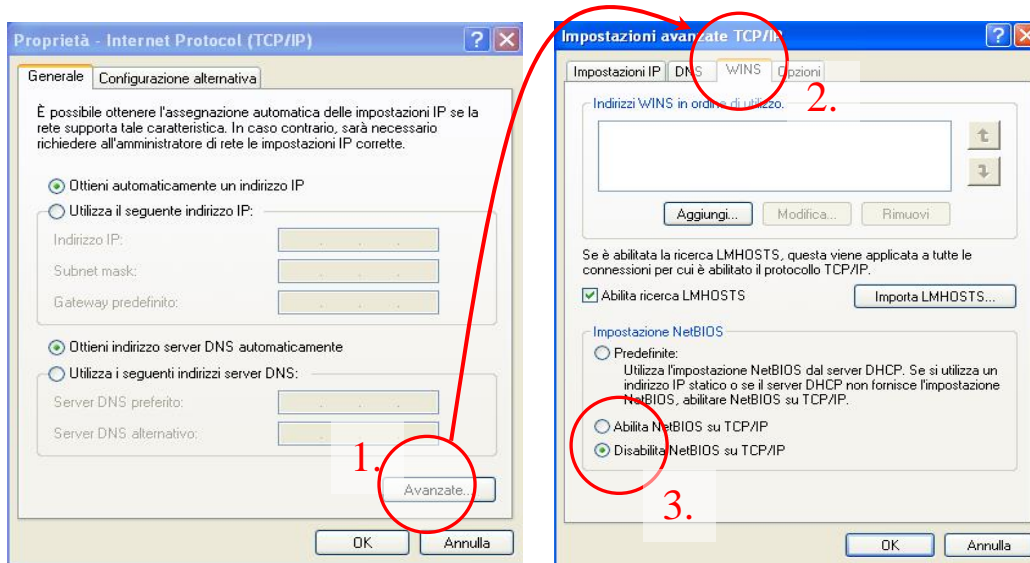


Illustrazione 22: disattivazione di NetBios su TCP/IP

Se non intendete o non potete rinunciare alla condivisione di file su Internet devono essere osservati alcuni punti. A titolo d'esempio la versione Home di Windows XP offre meno possibilità della versione Professional per quanto concerne la condivisione dei file. Per questo motivo si sconsiglia di massima la condivisione di rete nel caso di Windows XP Home.

Nel caso di Windows XP Professional sono disponibili più opzioni per la condivisione delle directory; nondimeno queste devono in precedenza essere rese accessibili, attivando in Esplora risorse il menu «Opzioni cartella → Visualizzazione».

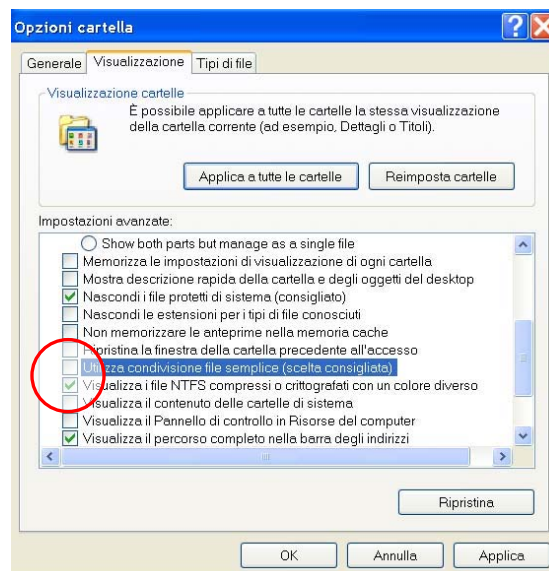


Illustrazione 23: disattivazione di «Utilizza condivisione file semplice»

Disattivando la selezione «Utilizza condivisione file semplice» si può accedere alla scheda «Protezione» nella proprietà delle directory e dei file (cfr. illustrazione 24) ed

è così possibile effettuare impostazioni specifiche per l'assegnazione di diritti di accesso.

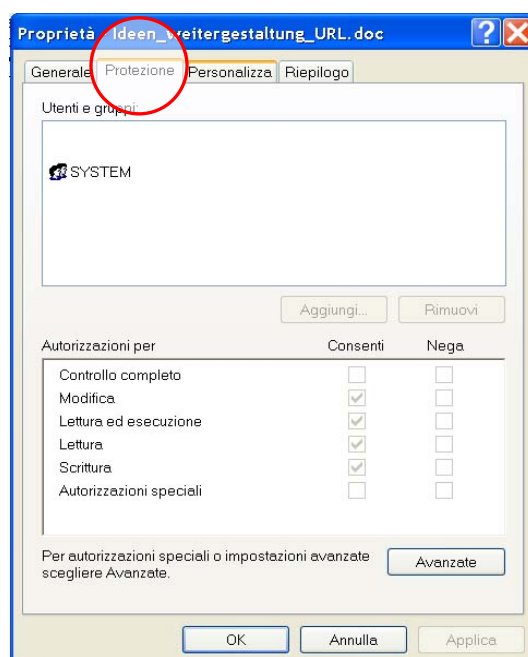


Illustrazione 24: definizione delle autorizzazioni in caso di condivisione

Blocco del desktop e salvaschermo

Chi sente la mancanza della combinazione di tasti Ctrl+Alt+Delete di Windows NT e di Windows 2000 per attivare il blocco del desktop, può ripristinarla per il tramite delle impostazioni già discusse al capitolo «Gestione dei conti di utente».

Verifica della sicurezza di sistema per il tramite di tools

Microsoft Baseline Security Analyzer (MBSA)

Per verificare in genere la sicurezza di sistema e in particolare quella delle impostazioni effettuate, si raccomanda Microsoft Baseline Security Analyzer. Il programma può verificare sia sistemi locali, ossia il vostro sistema, sia sistemi distanti. Microsoft fornisce informazioni di applicazione del tool al seguente indirizzo:

<http://support.microsoft.com/default.aspx?scid=kb;it;320454>

Reperimento e rimozione di spyware e di adware

Spyware e adware sono presenti su numerosi computer. Lo *spyware* è destinato a raccogliere all'insaputa dell'utente informazioni sulle sue abitudini di navigazione oppure sulle configurazioni di sistema per trasmetterle a un indirizzo predefinito. Il tipo di informazioni lette varia da uno spyware all'altro e può spaziare dalle abitudini di navigazione sino alle password. Il concetto di *adware* deriva dall'unione delle parole inglesi *advertising* (pubblicità) e *software*. È difficile stabilire una chiara delimitazione tra le definizioni di spyware e di adware. In genere l'adware è utilizzato piuttosto a scopi pubblicitari, nel senso che le abitudini di navigazione dell'utente vengono registrate e sfruttate per offrirgli prodotti corrispondenti (ad es. per il tramite di link).

Lo spyware e l'adware si installano solitamente sul computer quando si scaricano programmi. La pagina Web di MELANI elenca tools per il loro reperimento e la loro rimozione.

http://www.melani.admin.ch/gefahren-schutz/links/index.html?lang=it#sprungmarke2_12

Questi tools (strumenti) non costituiscono nondimeno un biglietto gratuito di navigazione spensierata in Internet, perché anche gli strumenti più efficaci non sono in grado di reperire e di rimuovere tutti i parassiti.

Riferimenti e link su informazioni complementari

- [1] Pagina di aggiornamento di MS Office
<http://office.microsoft.com/it-it/officeupdate/default.aspx>

- [2] Protezione contro pericoli e rischi
<http://www.melani.admin.ch/gefahren-schutz/schutz/index.html?lang=it>

- [3] Link su software antivirus
http://www.melani.admin.ch/gefahren-schutz/links/index.html?lang=it#sprungmarke2_4

- [4] Salvaguardia dei dati
<http://www.melani.admin.ch/gefahren-schutz/schutz/00034/index.html?lang=it>

- [5] Impostazione dei criteri di controllo
<http://www.microsoft.com/italy/technet/security/guidance/secmod62.msp#EIAA>

- [6] Service Guide per Windows XP (inglese)
http://www.theeldergeek.com/services_guide.htm

- [7] Link su personal firewall
http://www.melani.admin.ch/gefahren-schutz/links/index.html?lang=it#sprungmarke2_5

- [8] Utilizzazione del sistema di crittografia dei dati (EFS)
<http://support.microsoft.com/default.aspx?scid=kb;it:307877>
<http://support.microsoft.com/kb/223316/> (inglese)

- [9] Crittografia dei dati dei dischi rigidi sotto Windows XP (tedesco)
<http://www.fz-juelich.de/zam/files/docs/tki/tki-0397.pdf>

- [10] Microsoft Baseline Security Analyzer
<http://support.microsoft.com/default.aspx?scid=kb;it:320454>

- [11] Strumenti in tema di «spyware» e «adware»
http://www.melani.admin.ch/gefahren-schutz/links/index.html?lang=it#sprungmarke2_12

- [12] Guida per la protezione di Windows XP
<http://www.microsoft.com/italy/technet/security/guidance/secmod62.msp>

- [13] Windows XP Security Guide (inglese)
<http://www.microsoft.com/technet/security/prodtech/winclnt/secwinxp/default.msp>

Allegato A: Determinazione del service pack installato

Il menu «Pannello di controllo → Sistema» indica il service pack installato (attualmente SP2).

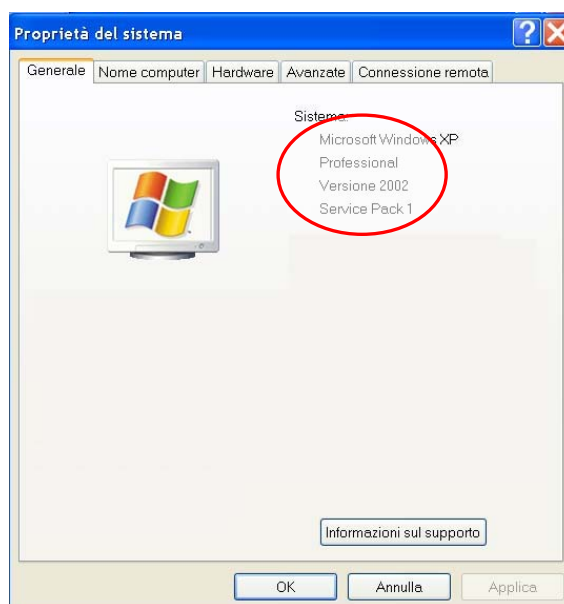


Illustrazione 25: reperimento del service pack installato

Allegato B: Visualizzazione delle informazioni sul filesystem

Le informazioni sul filesystem di un supporto di dati possono essere visualizzate come segue:

- 1.) Aprite Esplora risorse
- 2.) Posizionate il cursore del mouse sul corrispondente supporto di dati (ad es. C:)
- 3.) Azionate (nella maggior parte dei casi) il tasto destro del mouse e selezionate il menu «Proprietà»
- 4.) Nella scheda «Generale» è visibile il filesystem utilizzato (cfr. illustrazione 26).

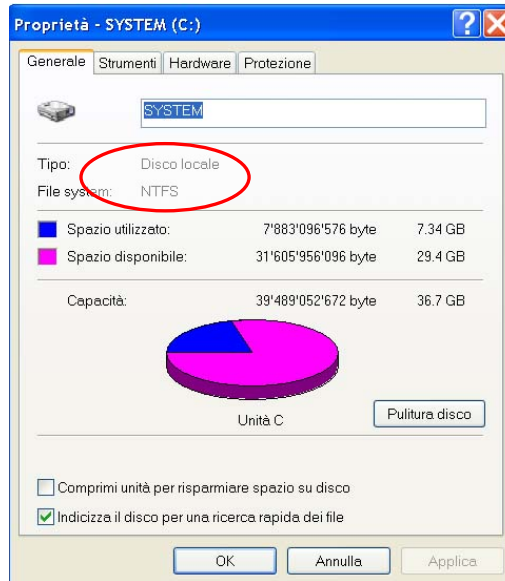


Illustrazione 26: informazioni sul filesystem