FermoLUG News

La Newsletter del FermoLUG Febbraio 2017 - Numero 15

Indice

Prendilo, è gratis (la prima volta)/2 1
Aggiornamenti software non pervenuti? 2
Cos'ha comprato Microsoft? 4

Gli aggiornamenti Microsoft..

In quanti sono in regola, dopo che Microsoft ha interrotto la distribuzione degli aggiornamenti? Le Pubbliche Amministrazioni, ad esempio, devono garantire le misure minime di sicurezza, tenendo tutti i Sistemi Operativi dei loro PC aggiornati..

Pagina 2

Linkedin è di Microsoft

Che vi piaccia o no i vostri dati registrati in Linkedin sono passati ora a Microsoft, senza esserne affatto informati. Quali interessi si celano dietro a questa raccolta dati costata più di 26 miliardi di dollari?

Pagina 4

Autori cercasi!

Se ti piace scrivere articoli e recensioni, FermoLUG News ti sta cercando! Invia il tuo materiale a:

info@linuxfm.org

Microsoft Azure gratuito.. ma chi ci guadagna veramente?

Prendilo, è gratis (la prima volta)/2

Se uno ha imparato a contare soltanto fino a sette
vuol mica dire che l'otto non possa esserci.
Jovanotti

Delle recenti strategie di marketing messe in atto dalle major del software, che regalano prodotti e servizi alle scuole nella speranza di formare futuri utenti paganti, abbiamo già parlato qui (http://www.techeconomy.it/2016/02/15/prendilo-gratis-la-volta).

Ovviamente anche le università rientrano in questi piani commerciali. Microsoft, ad esempio, ha lanciato il suo programma **Microsoft Educator Grant** (https://www.microsoftazurepass.com/azureu), destinato ai docenti universitari e ai loro studenti. Il programma offre accesso gratuito ai servizi cloud Microsoft Azure per il docente e gli allievi del suo corso. Secondo le intenzioni di Microsoft "il programma Microsoft Educator Grant nasce con l'obiettivo di dare ai professori e agli studenti nel contesto universitario l'opportunità di sfruttare tutti i vantaggi di Microsoft Azure, usufruendo, in ambito didattico, di una piattaforma di servizi cloud avanzata come quelle utilizzate dalle grandi aziende".

Dato che normalmente l'account di accesso a Microsoft Azure viene venduto a 250 dollari al mese per il docente e a 100 dollari al mese per ogni studente, sembra un'ottima cosa.

Invece no. Per diverse ragioni:

1. l'account **docente è gratis solo per un anno**, gli account **studente addirittura solo per sei mesi**; alla scadenza bisognerà pagare i canonici 250 $/mese e i 100 $/mese per mantenerli attivi. Se non si provvede entro 90 giorni, tutti i dati verranno semplicemente eliminati. In realtà è abbastanza verosimile che, trattandosi di strumenti messi in piedi a scopo didattico, dopo un semestre uno studente non ne abbia più bisogno, come non ne ha bisogno il docente dopo un anno, ma a chi piacerebbe sapere che il materiale con cui hai preparato un esame sta per sparire per sempre e non potrà più essere usato né consultato, se non pagando cifre non propriamente trascurabili?
2. **l'università non è un'azienda privata**, ma è l'istituzione che fa della condivisione della conoscenza, insieme alla ricerca scientifica,

uno dei fondamenti della sua esistenza. La condivisione della conoscenza non si può avere se non in un contesto di neutralità tecnologica (o almeno di pluralismo) e di utilizzo di standard aperti. Può la conoscenza essere rinchiusa in "scatole" private e disponibile addirittura a tempo determinato? Che succederebbe se lo stesso destino di quei dati, cancellati dopo un anno, fosse riservato – per dire – anche alle biblioteche universitarie, così ricche di saperi, in molti casi secolari, liberamente accessibili a chiunque?

3. **chi ci guadagna veramente da questa offerta?** Gli studenti? Non molto: avere imparato ad usare uno strumento tra i tanti, proprietari e liberi, che il mercato propone, solo perché regalato, in generale non è un buon biglietto da visita da presentare sul mercato del lavoro. I Docenti? Forse: la disponibilità di una soluzione bell'e pronta e che non grava sulle casse sempre troppo vuote degli atenei è una tentazione troppo forte, ma lascia aperti gli interrogativi posti al punto precedente. Chi propone l'offerta? Sicuramente: uno studente (non pagante) che si forma su un dato strumento sarà portato a pensare che quello sia l'unico esistente, o comunque il migliore sul mercato, e sarà quindi un probabile futuro utente (pagante) di quello strumento, anche semplicemente perché lo sa già usare.

Ma è davvero quello che vogliamo?

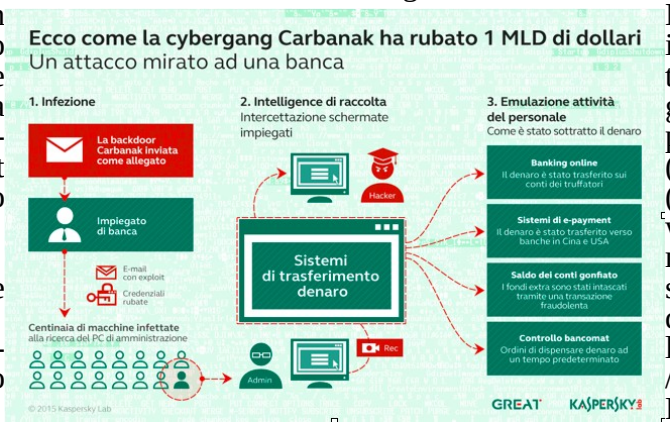
- Marco Alici - Fonte: http://www.techeconomy.it/2016/04/15/prendilo-gratis-la-volta-2/

Aggiornamenti software non pervenuti?

Era marzo 2013 quando la nostra redazione pubblicava la notizia (http://www.techeconomy.it/2013/03/25/internet-record-in-australia-per-la-prima-volta-a-1-000-mld-di-bit-al-secondo/) che in Australia nel collegamento tra Sydney e Melbourne veniva battuto il record mondiale di velocità su internet, con un traffico dati che viaggiava a mille miliardi di bit al secondo (un terabit/s).

Era invece gennaio 2016 quando proprio l'**ospedale di Melbourne** (la seconda città Australiana per numero di abitanti), era vittima di un grave attacco malware ad opera del **QBot Virus**, un worm che sfrutta una vulnerabilità di **Windows XP** e che ha tenuto impegnato per molte ore tutto il personale dell'Ospedale mettendo a rischio le informazioni sensibili dei malati ed il funzionamento dei macchinari medici.

E sempre nei primi mesi di quest'anno un altro grave episodio (https://blog.kaspersky.it/carbanak-colpo-da-1-miliardo-di-dollari/5622/) balzava alla cronaca, quello che è stato battezzato come il "**cyber-attacco bancario del secolo**", ossia la campagna hacker chiamata **Carbanak** che ha fruttato ai criminali che l'hanno messa in atto un miliardo di dollari. Tale attacco pur sfruttando gli Advanced Persistent Threats, o APT (http://www.techeconomy.it/2015/11/10/abc-sicurezza-advanced-persistent-threat/), non si basava su vulnerabilità zero-day (http://www.techeconomy.it/2015/11/17/abc-sicurezza-zero-day/), ma su bug conosciuti, approfittando di sistemi non aggiornati, vulnerabili e imprudenza degli utenti.



Nel 2011 il "Security Intelligence Report (SIRv11)" (http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf) di Microsoft riportava che solo l'uno per cento degli exploit, nella prima metà dell'anno, ha sfruttato vulnerabilità zero-day. Il resto dei problemi è dovuto in gran parte a **sistemi non aggiornati e ad attività di social engineering**. Dal 2011 ad oggi però poco è cambiato se nel Rapporto Clusit 2015 (http://www.clusit.it/download/Rapporto_Clusit%25202015.pdf) si legge " .. ancora nel primo semestre 2015 le vulnerabilità note e le tecniche di attacco più banali, ovvero più facili da contrastare, sono quelle che hanno causato più incidenti". Infatti come si vede dalla tabella qui sotto, mentre gli attacchi "zero-day" rispetto al 2014 hanno avuto un forte calo, le vulnerabilità note e gli SQL Injection (quindi database dei siti web non aggiornati) sono in crescita. Lo stesso Report Annuale sulla Sicurezza Cisco del 2015 (http://www.cisco.com/web/IT/offers/lp/2015-annual-security-report/index.html) afferma che i portali web (CMS – Content Management System) fanno parte dei sistemi più attaccati (11% del totale).

Distribuzione delle tecniche di attacco per tipologia

TECNICHE DI ATTACCO	2011	2012	2013	2014	2012 su 2011	2013 su 2012	2014 su 2013	2H 2014	1H 2015	1H 2015 su 2H 2014	Trend 2015
SQL Injection	197	435	217	110	120,81%	-50,11%	-49,31%	54	103	90,74%	↑
Unknown	73	294	239	199	302,74%	-18,71%	-16,74%	98	111	13,27%	↑
DDoS	27	165	191	81	511,11%	15,76%	-57,59%	35	41	17,14%	↑
Vulnerabilità note	107	142	256	195	32,71%	80,28%	-23,83%	91	103	13,19%	↑
Malware	34	61	57	127	79,41%	-6,56%	122,81%	62	54	-12,90%	→
Account Hijacking / Theft	10	41	115	86	310,00%	180,49%	-25,22%	37	56	51,35%	↑
Phishing / Social Engineering	10	21	3	4	110,00%	-85,71%	33,33%	0	3	300,00%	↑
Multiple Techniques / APT	6	13	71	60	116,67%	446,15%	-15,49%	52	46	-11,54%	→
0-Day	5	8	3	8	60,00%	-62,50%	166,67%	5	0	-500,00%	↓
Phone Hacking	0	3	0	3	-	-	-	2	0	-200,00%	↓

© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia (aggiornamento al 30 giugno 2015)

Il dato che ne risulta è che nonostante la tecnologia faccia passi da giganti, l'Internet of Thing stia diventando quotidianità, la tecnologia Smart e Wearable un qualcosa che ci fa restare connessi in ogni luogo, la questione degli aggiornamenti e dei sistemi sicuri è un qualcosa che sentiamo ancora lontana.

WINDOWS XP

Sappiamo benissimo che il supporto e gli aggiornamenti di Windows XP sono scaduti ad aprile 2014 e che il suo antivirus non è più aggiornato da luglio 2015, ma nonostante ciò ancora oggi **Windows XP è presente per il 10,9%** dei sistemi operativi utilizzati, di poco sopra a Windows 8.1 (9,56%), sotto a Windows 10 (14,15%) e Windows 7 (51,89%) (fonte: *netmarketshare.com*).

Windows XP è presente in molte aziende, in molti uffici e strutture pubbliche, in molti ospedali. Interessante a tal proposito l'analisi e l'esperimento riportato su questo articolo (http://www.techeconomy.it/2015/09/17/usare-windows-xp-dormire-preoccupati/) da Paolo Giardini. Come vedete a fronte di 128 documenti scaricati dal sito "governo.it" e dall'analisi dei suoi metadati, 31 file riportavano l'indicazione dei sistemi operativi con i quali erano stati prodotti. E di questi 31 ben 16 provenivano da Windows XP.

Ho voluto replicare l'esperimento per attualizzarlo ed integrarlo. Ho provveduto ad analizzare i metadati dai documenti scaricati dal sito **comune.venezia.it**, altro grosso ente pubblico. Delle centinaia di documenti scaricati, 90 mi hanno permesso di estrarre il sistema operativo con cui sono stati prodotti/modificati. La situazione che è comparsa è la seguente: 34 Windows XP, 50 Windows Server 2000, 3 Windows 98, 1 Mac OS, 2 Windows NT 4.0. I dati incredibili parlano da soli.

Restando in tema di Windows XP desidero fare una precisazione: gli sportelli bancomat non hanno Windows XP classico come lo conosciamo noi. Moltissimi hanno invece un sistema operativo basato sul Kernel di Windows XP ma chiamato **Windows Embedded POSReady 2009** che viene appunto installato su postazioni Bancomat, macchine compatte, registratori di cassa. E proprio per l'uso che ne viene fatto a questo sistema Microsoft concede la possibilità di ricevere gli aggiornamenti fino al 09 Aprile 2019 (https://support.microsoft.com/en-us/lifecycle?p1=14086). Pur non essendo una procedura supportata e autorizzata da Microsoft (ovviamente :-D), è stata trovata una tecnica che attraverso una modifica al Registro di Sistema di Windows XP SP3, permette anche ad esso di ricevere gli aggiornamenti di sicurezza fino al 2019 come se si trattasse di Windows Embedded POSReady. Essendo comunque i due sistemi diversi la procedura non è esente dal creare instabilità al sistema in talune condizioni.

WINDOWS SERVER 2003

Il 14 luglio 2015 è terminato il supporto di Microsoft a Windows Server 2003 e Windows Server 2003 R2. Molto importante anche questo aspetto perché qui si tratta di sistemi operativi server, che come tali si trovano a gestire i dati cruciali di un'azienda. Dati contabili, gestionali, database, configurazioni di rete, archivi documentali, tutte informazioni molto delicate e che nessuna azienda vorrebbe mai perdere che saranno vulnerabili se non si è migrati ad altro sistema operativo.

WINDOWS 7 e WINDOWS 10

L'importanza che deriva dall'avere sempre sistemi e programmi aggiornati è anche visibile nella gestione degli aggiornamenti dei sistemi operativi di casa Microsoft da Windows 7 in poi. Questo infatti ha visto per gli utenti consumer l'update forzato al Service Pack 1, mentre ancora facoltativo per gli Amministratori di rete. Per quanto riguarda Windows 10, la versione Home installa obbligatoriamente gli aggiornamenti senza necessità del consenso utente. E' attivata la funzione di aggiornamento automatico che non può essere disattivata dagli strumenti di gestione del sistema. Per le altre versioni di Windows 10, di norma possedute dalle aziende, rimane la scelta in capo agli Amministratori di installare o meno i singoli aggiornamenti.

LEGISLAZIONE SULLA PRIVACY

Oltre all'aspetto della sicurezza, è importante considerare che sistemi operativi non aggiornati pongono le aziende in una condizione di violazione della normativa italiana sulla privacy, non garantendo più le misure minime di sicurezza.

CONSIGLI GENERALI

E' fondamentale tenere presente che mantenere tutti i sistemi aggiornati ci mette al riparo non solo da malware e criminali, ma anche da bug che creano instabilità e mal funzionamenti, guasti e violazioni della normativa sulla privacy. Dovremmo pertanto:

1. Utilizzare solo sistemi operativi e software originali e conformi alle normative
2. Aggiornare periodicamente ogni software installato su un sistema informatico, i singoli programmi, le applicazioni sugli smartphone, i driver ed i firmware delle periferiche. Impostare precise politiche aziendali che prevedano anche una verifica periodica degli aggiornamenti di ogni software e sistema. Non fidarsi di aggiornamenti automatici ma verificare verificare che i sistemi siano sempre aggiornati e nel caso non lo fossero aggiornare manualmente.
3. Non "Jailbreakkare" l'iPhone o effettuare il "root" sui dispositivi Android perché espone a problemi di sicurezza. Potendo scaricare app dagli store non ufficiali è possibile incappare e scaricare malware. Inoltre tali dispositivi potrebbero avere dei punti di accesso che in condizioni normali non avrebbero e rendere vulnerabile così il dispositivo per i criminali.
4. Scaricare sempre le app dagli store ufficiali e anche da questi scaricarle solo dopo aver preso informazioni da altri utenti o amici che già le utilizzano. Fare attenzione alle applicazioni che hanno il nome simile a quello che davvero si sta cercando perché potrebbero non fare quello che ci si aspetta. Verificare inoltre che il produttore del software sia davvero chi deve essere.
5. Non dimenticarsi dei device smart (Smartphone, SmartTV, ..) o dei Wearable o delle auto moderne.

Tutto quello che è connesso ad internet sicuramente avrà la possibilità e la necessità di essere aggiornato. - Antonio Sagliocca - Fonte: http://www.techeconomy.it/2016/04/06/aggiornamenti-software-non-pervenuti/

Cos’ha comprato Microsoft?

Appena uscita, la notizia (news.-microsoft.com/2016/06/13/microsoft-to-acquire-linkedin/) ha fatto subito il giro del mondo: Microsoft ha annunciato – a cose fatte – di aver comprato Linkedin (linkedin.com). Costo dell’operazione: poco più di 26 miliardi di dollari. In contanti. 26 miliardi di dollari sono un po’ più dell’1% del PIL dell’Italia, il doppio del PIL dell’Albania (www.google.it/publicdata/explore?ds=d5bncpp-jof8f9_&met_y=ny_gdp_mktp_cd&idim=country:ITA:FRA:ESP&hl=it&dl=it#%21ctype=c&strail=false&bcs=d&nselm=s&met_y=ny_gdp_mktp_cd&scale_y=lin&ind_y=false&idim=country:ITA:ALB&ifdim=country:region:ECS&pit=1402696800000&hl=it&dl=it&ind=false), una volta e mezzo il prezzo pagato nel 2014 da Facebook per Whatsapp.
Sulle motivazioni strategiche di questa acquisizione si è già detto (techeconomy.it/2016/06/15/microsoft-acquista-linkedin-punto/): Microsoft sta progressivamente disinteressandosi del mercato desktop e dell’utente domestico, accrescendo le sue attenzioni verso il mondo delle imprese e delle organizzazioni, e Linkedin è il maggiore social network orientato al mondo del lavoro. Non ci compete nemmeno fare analisi economiche per capire se Linkedin è uno strumento così tanto prezioso da valere 26 miliardi di dollari o se Microsoft ne aveva così tanto bisogno per il suo business da essere disposta a spendere qualunque cifra (e comunque stiamo tranquilli: se anche fossero soldi buttati, Microsoft non finirà sul lastrico per questo. Notizia (ilsole24ore.-com/art/finanza-e-mercati/2016-06-14/microsoft-compra-linkedin-debito-224520.shtml), anche questa, tutta da meditare). La domanda che ci poniamo è un’altra: cosa ha comprato Microsoft esattamente? Un’azienda con oltre 1500 dipendenti? Certamente. Un’infrastruttura hardware e software di tutto rispetto? Anche. Uno strumento per integrare nuove funzionalità da proporre ai propri clienti di prodotti per la produttività? Senz’altro. Ma davvero tutto questo vale da solo un punto di PIL italiano, o due PIL albanesi eccetera? Probabilmente con un decimo di quella cifra si sarebbe potuto mettere in piedi un’azienda e un’infrastruttura hardware e software di pari livello. Dunque dev’esserci dell’altro, e infatti c’è: con Linkedin Microsoft ha comprato anche (soprattutto?) i suoi 400 (quattrocento) milioni di utenti, che sono più degli abitanti degli USA, un terzo degli abitanti della Cina. Quattrocento milioni di profili, che sono dati anagrafici, curriculum, informazioni lavorative, ma anche dati aziendali, abitudini, interessi individuali e di gruppo e quant’altro possa esserci dentro al profilo utente di un social network. In altre parole: **informazioni sulle persone**. O meglio, informazioni su quattrocento milioni di persone. Poco importa che solo un quarto siano utenti attivi, l’attività non è tanto importante quanto le informazioni personali, materiale su cui Zuckerberg ha costruito la sua fortuna patrimoniale e il suo potere. Che siano le informazioni a giustificare la spesa? Certo, un utente che si era iscritto a Linkedin dando i suoi dati a un’azienda, di fatto li sta consegnando nelle mani di un’altra. A sua insaputa, peraltro. Non è la prima volta che succede: è accaduto agli utenti di Whatsapp, ma anche a quelli di Skype, di Instagram, e di chissà quanti “luoghi” in cui siamo entrati. Né sta a noi dire se la cosa sia buona o cattiva: di certo come utenti – “basic”, ma soprattutto “premium”, che pagano – avremmo il diritto di essere, se non proprio interpellati, almeno informati. Possibilmente prima degli azionisti. O è chiedere troppo? - (foto di Luca Biada Flickr, CC-BY 2.0) - Marco Alici - Fonte:techeconomy.it/2016/06/17/

Associazione Culturale
Fermo Linux Users Group
Gruppo Utenti Linux di Fermo
C.F.90037220440
www.linuxfm.org
info@linuxfm.org

Gruppo Telegram:
bit.ly/fermolug
Mailinglist pubblica:
http://liste.linuxfm.org/mailman/listinfo/discussioni

Il FermoLUG nasce nel 2003 da un gruppo di amici con la voglia di condividere le proprie scoperte in ambito informatico.

Lo scopo principale dell'Associazione è quello di promuovere e diffondere il Software Libero facendo corsi di formazione, eventi aperti a tutti e tenendo attiva e legata la propria comunità di soci e simpatizzanti.

Se hai voglia di condividere idee, trucchi e soluzioni nell'uso quotidiano di GNU/Linux, inserisciti nella Mailing List: è un sistema facile e veloce per entrare direttamente in contatto con i membri del LUG!

Se desideri aiutarci attivamente nella nostra missione, iscrivendoti ufficialmente alla nostra associazione, clicca su “Diventa Socio” dal nostro sito web www.linuxfm.org.
Il costo dell'iscrizione è di 10€.