Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – DICEMBRE 2015

****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità. E' possibile dare il proprio contributo e diffonderla a chiunque.

E' disponibile il blog http://blog.cesaregallotti.it.

E' possibile iscriversi o dis-iscriversi scrivendo a cesaregallotti@cesaregallotti.it o seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/Newsletter.html

Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****

Indice

****

00- Editoriale

Mi riservo un piccolo spazio a dicembre per fare gli auguri di buone feste a tutti i miei lettori.

Così faccio anche quest'anno e vi do appuntamento a gennaio 2016.

Questo numero è un po' più lungo degli altri perché ho voluto includere le ultime novità sul GDPR e per dare più letture a coloro che dovessero annoiarsi se la neve in montagna è troppo poca.

****

01- Regolamento europeo privacy - Aggiornamenti

La notizia è, credo, ben nota: il Regolamento europeo privacy (GDPR) ha fatto altri passi avanti. È stato concordato il testo da parte del "trilogo", ossia Commissione, Consiglio e Parlamento europeo.

Per quanto riguarda il percorso, Biagio Lammoglia, che ringrazio, mi ha scritto che: "i Triloghi (plurale, visto che gli appuntamenti sono stati molteplici) hanno prodotto un testo di accordo definitivo tra l'Istituzione proponente (Commissione Europea) e le Istituzioni legiferanti (Parlamento e Consiglio), che deve essere solo ratificato dal doppio passaggio nelle Camere competenti (Parlamento e Consiglio) in tempi certi (entro la Primavera)".

Biagio aggiunge anche: "Per quanto previsto ancora un doppio passaggio parlamentare (Parlamento e Consiglio), la prassi vuole che l'accordo raggiunto nelle fasi di Trilogo risolva in modo definitivo le controversie e che il testo risultante non possa più essere modificato in modo sostanziale (ad esempio la casistica che determina l'obbligo di adozione del DPO è stata ormai fissata)".

Un articolo in inglese che dettaglia il percorso ancora da fare (grazie a Pierfrancesco Maistrello di Vecomp):
- http://www.insideprivacy.com/international/european-union/political-agreement-on-the-eu-general-data-protection-regulation/.

Traduzione finale: se tutto ciò è vero, l'iter si concluderà non più tardi di fine marzo 2016. In questo modo, considerando il periodo di transizione di 2 anni, le organizzazioni dovranno adeguarsi entro la primavera del 2018.

Segnalo un articolo in italiano, che mi sembra molto equilibrato (da un tuit):
- http://www.webnews.it/2015/12/16/regole-riforma-privacy-europa/.

Un articolo in inglese, che mi sembra però meno equilibrato:
- http://techcrunch.com/2015/12/16/gdpr-agreed.

Un articolo in inglese di Biagio Lammoglia su Europrivacy.info (segnalati da Alessandro Vallega di Oracle):
- http://europrivacy.info/2015/12/16/the-agreement-has-been-reached-gdpr-is-under-christmas-tree/.

Un altro articolo in inglese, segnalatomi sempre da Pierfrancesco Maistrello di Vecomp, di provenienza USA (Pierfrancesco dice "trovo utili queste testimonianze da oltreoceano, perché ci danno l'idea di quale sia il loro focus su questo tema, non sempre coincidente con il nostro"):
- http://blogs.wsj.com/law/2015/12/16/the-eu-data-privacy-agreement-what-we-know-and-dont/.

I due link (grazie a @europrivacy) alle ultime bozze:
- regolamento: http://ow.ly/d/47uW.
- direttiva per il trattamento dei dati trattati a scopo investigativo: http://ow.ly/d/47v0.

Notate che in questo testo ci sono commi e articoli con puntini di sospensione. Evidentemente sono punti cancellati da bozze precedenti. Il tutto, ovviamente, verrà consolidato.

Cosa ne penso?

Penso che varrebbe la pena aspettare la pubblicazione del testo definitivo e qualche interpretazione "ufficiale" (Garante privacy, WP Art. 29, eccetera) su alcuni requisiti ora un po' vaghi.

Ai miei clienti proporrò di vederci in aprile, a Regolamento pubblicato e in occasione delle periodiche attività di aggiornamento e verifica, per fare una prima analisi delle cose da modificare e predisporre un piano per il 2016-2017.

Ho ancora la speranza che il nostro Garante privacy cerchi di aiutare le aziende con interpretazioni utili. Finora purtroppo non ha fatto alcunché, anzi, forse ha aumentato la confusione in merito a questo Regolamento, alimentando un mercato di pirati. Su questo punto vorrei scrivere di più, ma evito.

****

02- Legale - Conservazione e firme elettroniche (linee guida AgID e articolo)

AgID ha pubblicato le "Linee guida sulla conservazione dei documenti informatici":
- http://www.agid.gov.it/notizie/2015/12/10/conservazione-pubblicate-linee-guida-agid.

Plaudo all'iniziativa di rendere più comprensibili le norme in materia di conservazione e di firma elettronica-digitale.

Nei miei sogni, questo documento dovrebbe essere una guida "for dummies". Se questa è l'intenzione anche di AgID, allora c'è ancora molto da semplificare. In tutti i casi, da qualche parte bisogna pur cominciare e il documento è ancora in fase di sviluppo.

Ho letto con estremo interesse questa serie di articoli di Francesco Foglio in merito a firme elettroniche e Regolamento iIDAS e il loro impatto sulla normativa italiana:
- http://www.e-idas.org/ancora-sulle-firme-elettroniche/;
- http://www.e-idas.org/firme-elettroniche-e-regolamento-eidas-scenario-e-impatti-sulla-normativa-italiana-prima-parte/;
- http://www.e-idas.org/firme-elettroniche-e-regolamento-eidas-scenario-e-impatti-sulla-normativa-italiana-ultima-parte/.

Consiglio di leggerli nell'ordine da me suggerito, visto che il primo è introduttivo (anche se postato per ultimo, a seguito di una mia richiesta di aiuto).

****

03- Dlgs 231: l'ente risponde per non aver adottato misure di controllo idonee

Segnalo questo articolo di Filodiritto perché è la prima sentenza di applicazione del Dlgs 231 che leggo:
- http://www.filodiritto.com/news/2015/231-cassazione-penale-lente-risponde-per-non-aver-adottato-misure-di-controllo-idonee.html.

****

04- FSE: un articolo sul Regolamento tecnico

Dopo avere annunciato la pubblicazione del Regolamento tecnico in materia di fascicolo sanitario elettronico o FSE (http://blog.cesaregallotti.it/2015/11/dpcm-sul-fascicolo-sanitario-elettronico.html), segnalo questo articolo che fa il punto della situazione:
- http://www.altalex.com/documents/news/2015/11/23/fascicolo-sanitario-elettronico.

****

05- Standardizzazione: Correzioni a ISO/IEC 27001 e 27002

Sono stati pubblicati i technical corrigendum della ISO/IEC 27001 e 27002.

È bene discuterli brevemente. Segnalo che in passato avevo sottovalutato l'importanza del secondo corrigendum della ISO/IEC 27001; qui cerco di rimediare.

Il primo corrigendum, comune a ISO/IEC 27001 e 27002, riguarda l'inventario, la classificazione e trattamento degli "asset". In questi casi, al termine "asset" si è aggiunto il termine "informazioni". Spesso risultava ovvio al lettore che le "informazioni" erano incluse negli "asset", ma evidentemente non a tutti.

Il secondo corrigendum della ISO/IEC 27001 riguarda la Dichiarazione di applicabilità. Qui è importante perché ora la DdA non deve più riportare necessariamente i controlli dell'Annex A, ma "i controlli necessari" (insieme a giustificazione e stato di attuazione). L'Annex A deve essere usato solo per indicare e giustificare eventuali esclusioni dei suoi controlli. Sarà interessante vedere come tutto ciò sarà interpretato nella pratica.

Il secondo corrigendum della ISO/IEC 27002 riguarda un riferimento incrociato sbagliato. Al controllo 14.2.8 si fa riferimento al controllo 14.1.9, mentre bisognava fare riferimento al controllo 14.2.9.

****

06- Standardizzazione: novità famiglie ISO/IEC 20000 e 27000 (27010, 27013, 27017, 20000-10)

Sono state pubblicate le nuove versioni delle norme in oggetto.

La **ISO/IEC 27010:2015** ha titolo "Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications".
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=68427.

Di questa ho letto la versione precedente del 2012 e ho pensato fosse totalmente inutile. Non perderò tempo a leggermi anche questa, a meno che qualcuno non mi suggerisca diversamente.

La **ISO/IEC 27013** (versione del 2015) ha titolo " Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1" e riguarda, ovviamente, le relazioni tra due norme molto importanti:
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64138.

Io avevo fornito molti contributi alla versione precedente. Su questa non ci ho lavorato, né l'ho letta. Comunque si tratta di un adattamento della precedente versione alla nuova ISO/IEC 27001, quindi non penso ci siano novità rilevanti.

La **ISO/IEC 27017:2015** ha titolo "Code of practice for information security controls based on ISO/IEC 27002 for cloud services":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757.

Si tratta di un'estensione dei controlli della ISO/IEC 27002 (o dell'Annex A della ISO/IEC 27001). In alcuni casi sono fornite ulteriori indicazioni per i controlli già presenti nella ISO/IEC 27002, in altri casi sono aggiunti nuovi controlli.

Interessante è osservare che tutte le estensioni e i nuovi controlli sono presentati indicando cosa è applicabile al cliente e cosa al fornitore di servizi cloud.

Non mi sembra ci sia nulla di straordinario da segnalare. Questo standard potrà essere utile a coloro che vorranno ottenere un "attestato di allineamento" ad esso. Per studiare come assicurare la sicurezza dei servizi cloud è necessario leggere altri documenti (magari partendo da quelli gratuiti messi a disposizione dalla Cloud security alliance o dal NIST).

La **ISO/IEC 20000-10** (del 2015) ha titolo "Information technology - Service management - Part 10: Concepts and terminology":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=68673.

Dispiace vedere che una norma di "concetti e definizioni" sia venduta a 118 Franchi svizzeri.

****

07- Risk assessment: Vera 4.2 ITA

Ho pubblicato la versione italiana del mio foglio di calcolo per un Very easy risk assessment (VERA) relativo alla sicurezza delle informazioni.

La pagina web è questa:
- http://www.cesaregallotti.it/Pubblicazioni.html.

****

08- Linee guida di design per i siti web della PA

Da un tuit di @ilnesi, segnalo che AgID ha presentato le Linee Guida di design (inteso come rappresentazione grafica) per i siti web della pubblica amministrazione:
- http://www.agid.gov.it/notizie/2015/11/20/online-linee-guida-design-i-siti-web-pa.
- http://design.italia.it/.

Il mio commento è semplice: non si parla di sicurezza.

Forse qualcuno penserà che sono troppo concentrato su questo tema, ma non credo. Innanzi tutto, si parla di "protezione dagli errori" e di "accessibilità" e quindi si poteva parlare anche di sicurezza. Inoltre, la sicurezza deve entrare nella rappresentazione grafica; a me vengono in mente le seguenti caratteristiche: rendere chiare le modalità di registrazione e di accesso, rendere chiaro quando un utente ha acceduto o meno all'area riservata con le proprie credenziali, rendere sempre disponibile un pulsante di disconnessione (e chiarire cosa succede se qualcuno chiude il browser senza usarlo).

Ovviamente si potrebbe cogliere l'occasione per approfondire i temi della sicurezza trattando di funzionalità e meccanismi tecnologici, ma forse questo sarebbe veramente troppo fuori tema.

Invito però i tecnici con le competenze opportune a fornire contributi ad AgID (io l'ho fatto con il testo di questo articoletto). Si tratta di una bella occasione.

****

09- Strategie nazionali e europee sulla sicurezza informatica

Ho letto il documento "Il Futuro della Cyber Security in Italia: Un libro bianco per raccontare le principali sfide che il nostro Paese dovrà affrontare nei prossimi cinque anni" del Laboratorio Nazionale di Cyber Security e del Consorzio Interuniversitario Nazionale per l'Informatica:
- https://www.consorzio-cini.it/index.php/it/labcs-home/libro-bianco.

Innanzitutto grazie a Fabio Teoldi che mi ha spinto a leggerlo. Purtroppo non mi è piaciuto. Dico "purtroppo" perché si tratta di un'occasione sprecata, se escludiamo il beneficio di visibilità data ai 52 autori.

Mi limito a commentare le raccomandazioni.

La prima raccomandazione è di "centralizzare competenze e responsabilità relative specificamente alla sicurezza cibernetica". Questa raccomandazione però non è accompagnata da un'analisi dei limiti dei CERT già presenti in Italia e del mandato dell'Agenda digitale europea. Tra l'altro, promuovere un ulteriore ente italiano, quando quelli già presenti hanno difficoltà di reperimento di personale competente, mi sembra difficile. Avrei voluto leggere un'analisi più approfondita.

La seconda raccomandazione è "la razionalizzazione dei data center della PA", sicuramente auspicabile. Ancora una volta, però, il documento è carente di analisi sulla situazione attuale e sulle iniziative oggi già in atto.

La terza raccomandazione riguarda la formazione. Innanzitutto e inspiegabilmente non tratta di scuole elementari e medie. In secondo luogo la proposta manca completamente di analisi e di profondità, limitandosi ad indicazioni estremamente banali.

Ultima raccomandazione riguarda le "Certificazioni, Best Practices e Framework di Sicurezza Nazionale" e ancora una volta non si trova un'analisi di quello che c'è (solo un accenno al fatto che esistono UNI e UNINFO per la normazione, nessun accenno ad Accredia e agli schemi da essa promossi o ad altri schemi), né una reale giustificazione per promuovere un ennesimo schema.

Mi spiace aver scritto un ennesimo articolo polemico (ho anche chiesto conferma ad un professionista che mi ha chiesto di rimanere anonimo) e forse, a sua volta, inutile.

Sempre il Consorzio interuniversitario nazionale per l'informatica ha pubblicato la prima bozza del "Framework Nazionale per la Cyber Security" e chiede commenti:
- https://www.consorzio-cini.it/index.php/it/labcs-home/labcs-news/934-consultazione-pubblica-framework-nazionale-per-la-cyber-security.

Parto dalle cose buone: questo framework si basa su quello del NIST, che è fatto molto bene. Inoltre propone un insieme di misure minime per le PMI.

La cosa cattiva è in realtà una sola e l'ho già detto: un "framework nazionale" non serve a nulla visto che viviamo in un contesto internazionale (spero poi qualcuno noti l'ironia involontaria nell'uso di anglismi, sin dal titolo, in un documento "nazionale").

Tra l'altro, l'Italia sta già promuovendo l'uso di una norma internazionale come la ISO/IEC 27001. Perché, se continuiamo a dire che il tema è poco diffuso, si cerca di promuovere altre cose che fanno solo confusione? Forse perché "sicurezza delle informazioni" è meno sexy di "cyber-security"?

Francamente non saprei.

Mentre io criticavo queste iniziative italiane, l'Europa si sta muovendo (grazie a retuit di @Silvia_Mar_).

Si tratta ancora di annunci, ma li fornisco per completezza (il primo è in italiano, gli altri in inglese):
- http://www.techeconomy.it/2015/12/08/ue-ce-laccordo-cybersecurity-paesi-richieste-strategie-nazionali-collaborazione/;
- http://ec.europa.eu/commission/2014-2019/oettinger/blog/first-eu-wide-legisation-cybersecurity-agreed_en;
- http://www.europarl.europa.eu/news/en/news-room/content/20151207IPR06449/html/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity.

****

10- Sviluppo sicuro (guide e studi)

Qualche documento relativo allo sviluppo sicuro.

1- "Website Security for Dummies" di WhiteHat Security Europe: http://go.whitehatsec.com/HY002010Lm1WZI60YdB00zP;
2- "Securing the SDLC for Dummies" di di WhiteHat Security Europe: http://go.whitehatsec.com/s0yZ0Yd0WBL00Y016m20P0I.

Mi sembrano librini di base, che dovrebbero essere studiati a memoria da quanti sviluppano.

3- "Minimizing code defects to improve software quality and lower development costs" di IBM: ftp://ftp.software.ibm.com/software/rational/info/do-more/RAW14109USEN.pdf.

Studio dell'ottobre 2008 che riporta una delle dichiarazioni più famose della sicurezza ("identificare un difetto del software dopo la consegna costa 30 volte in più che farlo in fase di progettazione") e quindi può essere usata come autorevole fonte. Poi non si capisce bene come sia stato calcolato questo valore, ma se lo ha inventato IBM è sicuramente più veritiero che se lo avessi inventato io.

4- Strumento di Threat modeling di Microsoft: http://www.microsoft.com/en-ca/download/details.aspx?id=42518.

Confesso che non ho mai visto usare strumenti di Threat modeling per lo sviluppo del software. Questo è gratuito. Mi piacerebbe ricevere contributi (da chi li ha usati realmente, la pura teoria non mi interessa):

Questi ultimi due link li ho ricavati da un articolo dell'ISACA Journal, volume 4 del 2015, dal titolo "Three Ways to Simplify Auditing Software Security Requirements and Design".

5- "Mobile Development Best Practices" di NowSecure: https://www.nowsecure.com/resources/secure-mobile-development/.

Non riesco a capire se si tratta di una buona guida, viste le mie diffuse incompetenze tecniche di programmazione mobile. Da una parte vedo che sono discussi molti casi da considerare, dall'altra non mi sembra che le "soluzioni" siano completamente sviluppate.

Infine segnalo l'articolo di DarkReading "The Programming Languages That Spawn The Most Software Vulnerabilities" che tratta dei linguaggi di programmazione il cui uso porta ad avere maggiori vulnerabilità:
- http://www.darkreading.com/vulnerabilities---threats/the-programming-languages-that-spawn-the-most-software-vulnerabilities/d/d-id/1323397.

In altre parole, PHP e ASP Web non hanno un numero maggiore di vulnerabilità, ma sono usati peggio degli altri. In realtà, Java e .NET dispongono di funzionalità proprio per ridurre le vulnerabilità, mentre questi no. Viene ovviamente naturale pensare che è sempre più necessario l'uso di analizzatori del codice prima di attivarlo in produzione.

Questo e altri dettagli si trovano nel "State of Software Security Report" di Veracode (che confesso di non aver letto):
- https://info.veracode.co.uk/state-of-software-security-report-volume6-pt2.html.

****

11- Perché i progetti IT falliscono

Colgo l'occasione di un interessante articolo dell'ISACA Journal volume 5 del 2015 dal titolo "Auditors and Large Software Projects".

In questo articolo si fa riferimento ad una pubblicazione di Intosai (Issue 26 del 2008) dal titolo "Why IT projects fail". Qui trovo interessante il contributo dell'Oman, che elenca i 21 rischi (intesi un po' come minacce, un po' come vulnerabilità) di project management. Ho trovato interessante leggerli e penso sia un buon riferimento per quando mi chiedono "cosa intendi per rischi di progetto?".

Per chi volesse leggere l'articolo:
- http://www.intosaiitaudit.org/intoit_articles/26_p12top17.pdf.

Le pubblicazioni di Intosai fino al 2010 si trovano qui:
http://www.intosaiitaudit.org/publication_and_resources/1.

****

12- IoT: Guida ENISA e un buffo incidente

Segnalo questa guida dell'ENISA dal titolo "Security and Resilience of Smart Home Environments: Good practices and recommendations":
- https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices.

L'ho scorsa molto velocemente, ma mi è sembrata completa e ben fatta.

Credo che questa notizia (tratta da Crypto-gram di dicembre) sia veramente interessante per capire gli impatti del IoT:
- http://www.zdnet.com/article/car-calls-911-after-alleged-hit-and-run-driver-arrested/.

In poche parole: una donna causa un incidente e fugge, l'automobile si accorge che c'è stato un incidente e chiama la polizia. Ovviamente la donna viene arrestata.

Il fatto che l'automobile chiami automaticamente la polizia è una misura di sicurezza nel caso in cui il guidatore sia coinvolto in un incidente e sia impossibilitato a fare la chiamata in autonomia. In questo caso, però, la misura di sicurezza si è dimostrata una misura contraria agli interessi (censurabili) del beneficiario.

****

13- Strumenti per gestire gli incidenti

Da un tuit di @bartblaze, segnalo una lista di strumenti e risorse per la gestione degli incidenti:
- https://github.com/meirwah/awesome-incident-response.

Non ho le competenze per confermarne la validità. Ma ricordo una cosa fondamentale: non cercate di rispondere agli incidenti o di raccogliere dati a scopo legale se non ne avete le competenze!

****

14- Guida per hacker principianti

Da un tuit di @therebus, l'articolo molto interessante "Abbiamo letto la guida per hacker principianti di Anonymous":
- http://www.wired.it/gadget/computer/2015/11/23/guida-per-hacker-principianti-anonymous/.

La guida "The noob guide" si trova al seguente link:
- https://ghostbin.com/paste/jrr89.

****

15- Guida ENISA per il cloud

ENISA ha pubblicato una guida (in inglese) per le piccole e medie imprese che vogliono usare servizi cloud e dal titolo "Cloud Security Guide for SMEs":
- https://www.enisa.europa.eu/media/press-releases/enisa2019s-security-guide-and-online-tool-for-smes-when-going-cloud.

Trovo l'iniziativa interessante, soprattutto per quanto riguarda le questioni che dovrebbe porre un cliente al fornitore di servizi cloud.

Come sempre, faccio la solita domanda: perché si continuano a fare guide per l'uso di fornitori di servizi cloud e non per i fornitori di tutti servizi informatici? Soprattutto considerando che non vedo questioni non applicabili ai fornitori non-cloud. Inoltre, io continuo a vedere il rischio di aziende che controllano per bene i fornitori di servizi cloud, ma non gli altri, lasciando aperte vulnerabilità importanti (e non si tratta di un rischio teorico, dato che ho visto parecchi di questi casi).

****

16- Lo stato delle cyber-assicurazioni

Segnalo questo articolo (via tuit di @ylventures) dal titolo "The State of Cyber Insurance":
- http://www.networkworld.com/article/3005213/security/the-state-of-cyber-insurance.html.

L'autore ha fatto ricerche sul mercato delle "cyber-assicurazioni" e riporta le lezioni imparate:
- la proprietà intellettuale non è coperta da queste assicurazioni (quindi, deduco, si tratta di assicurazioni che coprono solo l'interruzione delle attività);
- le polizze possono essere fatte male, in quanto si tratta di un mercato "giovane";
- i prezzi sono alti perché i dati attuariali sono troppo limitati;
- i premi sono calcolati su valutazioni del rischio statiche e non dinamiche;
- le compagnie di assicurazione dovrebbero chiedere l'applicazione del NIST Cybersecurity Framework (l'autore, ovviamente, è degli USA);
- non ascoltate i venditori di prodotti "utili per ridurre i premi per le assicurazioni";
- in futuro ci saranno molte cause collegate ai pagamenti o mancati pagamenti da parte delle compagnie di assicurazione;
- il mercato migliorerà con gli anni.

Tutto molto interessante, ma, a fronte di una ricerca condotta per un anno, mi sarei aspettato qualche cosa in più:
- cosa si intende per "cyber-assicurazione"? Un'assicurazione che riguarda solo gli eventi relativi ad attacchi informatici da Internet, o anche quelli dall'interno; le cui liquidazioni si basano su quali parametri (tempi di interruzione e conseguenti perdite monetarie o altri aspetti)? Ovviamente, come al solito, qui si usa il termine "cyber" a casaccio;
- si parla del mercato delle "cyber-assicurazioni", ma non si specifica quanto è stato liquidato, quante richieste di liquidazione sono state fatte e quante sono state respinte, eccetera.

Peccato: un'occasione persa per fare vera informazione.

****

17- Un Windows 3.1 spegne l'aeroporto di Parigi

È brutto dare certe notizie in questi giorni, ma qui ci occupiamo di qualità e sicurezza delle informazioni (per i commenti e il dolore per le stragi del 13 novembre, altri hanno scritto meglio di me).

La notizia la ricavo dal SANS NewsBites e ha titolo "Failed Windows 3.1 system blamed for shutting down Paris airport":
- http://arstechnica.com/information-technology/2015/11/failed-windows-3-1-system-blamed-for-taking-out-paris-airport/.

Insomma, questi negli anni Novanta hanno installato un sistema critico su un pc con Windows 3.1 (e non su un AS/400 o simile) e da allora non l'hanno più aggiornato. Un aeroporto... degli sviluppatori di sistemi critici... Non ho parole.