Cybersecurity, protezione dei dati personali e transizione digitale: opportunità e rischi. Prospettive e strategie per l'interesse nazionale.

AICA

59° Congresso

28 ottobre 2022

www.aicanet.it/congresso2022

« Promozione degli interessi nazionali e sovranazionali attraverso la cybersecurity »

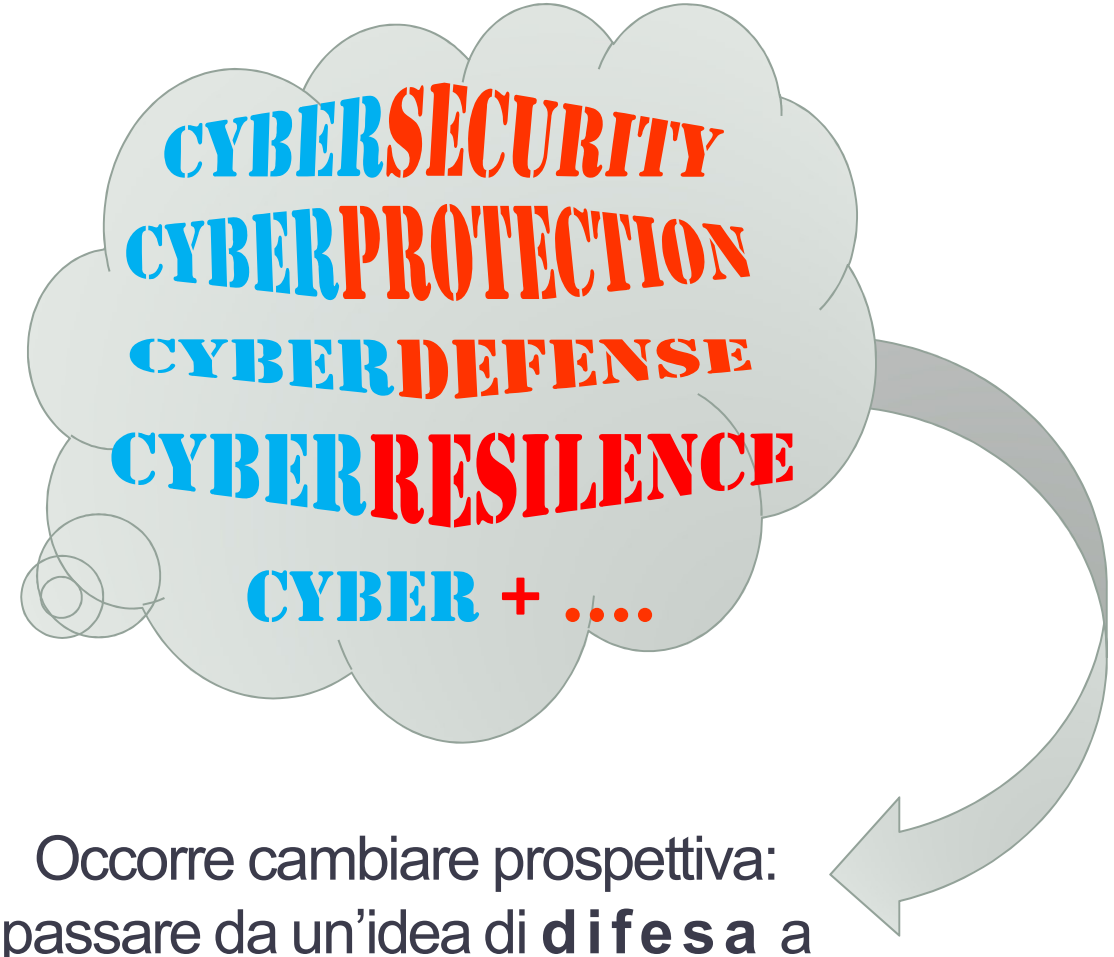
Carlo Muzzì

muzzi@acm.org

«Cybersecurity»: un cambio di prospettiva

La nostra mente associa il termine cybersecurity a prospettive tipicamente difensive.

È divenuto quasi un bias da sovvertire !



Occorre cambiare prospettiva: passare da un'idea di **difesa** a quella di **promozione** degli interessi strategici !

«Cybersecurity»: prospettive economiche

Technology Markets

Cybersecurity - Worldwide

Worldwide

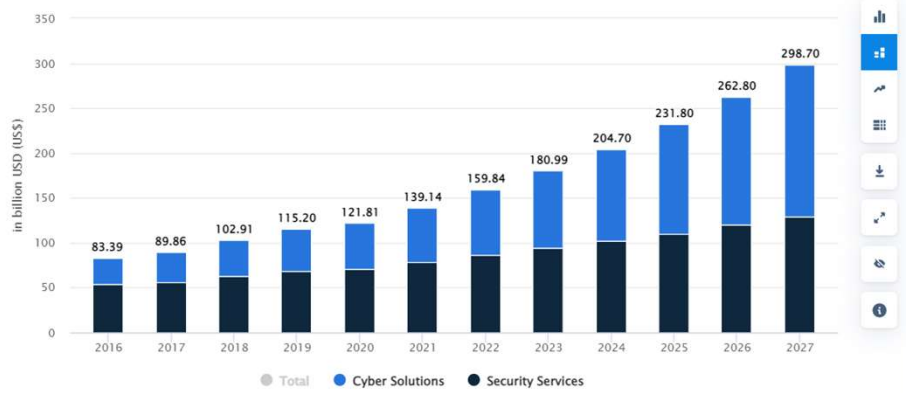
HIGHLIGHTS | MARKET DEFINITION | IN-SCOPE / OUT-OF-SCOPE | REPORTS

- Revenue in the Cybersecurity market is projected to reach US$159.80bn in 2022.
- The market's largest segment is Security Services with a projected market volume of US$86.26bn in 2022.
- Revenue is expected to show an annual growth rate (CAGR 2022-2027) of 13.33%, resulting in a market volume of US$298.70bn by 2027.
- The average Spend per Employee in the Cybersecurity market is projected to reach US$7.50k in 2022.
- In global comparison, most revenue will be generated in the United States (US$64,860.00m in 2022).

Market: Cybersecurity | Region: Worldwide | Compare to other regions +

Revenue

REVENUE BY SEGMENT



Notes: Data shown is using current exchange rates and reflects market impacts of the Russia-Ukraine war.

Most recent update: Jul 2022

Sources: Statista, Financial Statements of Key Players, National Cyber Security Organizations

ESTRATTO DA: https://www.statista.com/outlook/tmo/cybersecurity/worldwide

osservatori.net digital innovation

Cerca

Home | Ricerche | Prodotti | Eventi | Community | Chi Siamo

Home › Comunicati stampa › Boom del mercato cybersecurity in Italia: 1,55 mld €, +13%

Boom del mercato cybersecurity in Italia: 1,55 mld €, +13%

L'interesse verso la cybersecurity è ai massimi storici, fra imprese e istituzioni

Cyber Security in Italia: i messaggi chiave

- Boom del mercato della **cybersecurity**: 1,55 mld di euro, +13%
- Crescono ancora gli attacchi cyber per un terzo delle imprese
- In Italia la spesa in cybersecurity è l'0,08% del PIL, ultimo posto tra i Paesi del G7
- Per oltre metà delle imprese serve rafforzare la sensibilizzazione del personale sui comportamenti
- Il 46% si è dotata di un Chief Information Security Officer per la sicurezza informatica

ESTRATTO DA: https://www.osservatori.net/it/ricerche/comunicati-stampa/cybersecurity-italia-mercato-crescita.

Una premessa: il peso economico è significativo, ma vedremo che quello strategico lo è di più.

«Lois de programmation militaire» per il periodo 2014-2019

ESTRATTO DA: https://www.defense.gouv.fr/dgris/politique-defense/lois-programmation-militaire#:~:text=La%20loi%20de%20programmation%20militaire%20est%20la%20premi%C3%A8re%20d%C3%A9clinaison%20concr%C3%A8te,sur%20la%20p%C3%A9riode%202014%2D2019.

«Lois de programmation militaire» per il periodo 2014-2019

Les ressources financières de la programmation

Le renouvellement de nos équipements

Un effort au profit de la préparation opérationnelle

Un coup d'arrêt à la déflation des effectifs

La préparation de l'avenir

Priorité à l'Europe de la Défense

A la demande du Président de la République, les travaux d'actualisation de la loi de programmation militaire ont été avancés début 2015 afin de prendre en compte la nette dégradation de l'environnement stratégique et opérationnel constatée depuis 2013.

Le projet de loi de programmation militaire actualisée, prévoyant un accroissement des crédits de 3,8 Mds€ d'ici à 2019 par rapport à la programmation initiale, a été voté et promulgué à l'été 2015, en vue d'une prise en compte des mesures (effort budgétaire, non-déflations d'effectifs, priorités capacitaires…) dès le budget de Défense 2016.

Puis, à la suite des attentats du 13 novembre 2015, le Président de la République a entendu apporter les réponses adaptées à l'existence de menaces se matérialisant par des actes de guerre perpétrés sur le sol national, en même temps qu'au besoin d'accélération des actions offensives sur les théâtres d'affrontements avec Daech et Al Qaïda. Il a annoncé, dès le 16 novembre devant le Congrès, l'arrêt de la diminution des effectifs du ministère des Armées jusqu'en 2019 avec l'objectif de renforcer les unités opérationnelles, la cyberdéfense et le renseignement et l'intensification de « l'effort de guerre » au Levant. Ces orientations ont été traduites à l'occasion du Conseil de défense du 6 avril 2016, en termes de financement additionnel, de politique de ressources humaines et de nouvelles capacités militaires. Il convenait aussi de prendre la mesure du niveau d'engagement élevé et durable des armées françaises et des moyens de la défense nationale, à raison de la simultanéité des opérations extérieures indispensables, dans le cadre de la stratégie de contre-terrorisme et du déploiement des forces sur le territoire national, pour la protection rapprochée de la France et des Français.

Sembra prevalere l'usuale visione difensiva della cyberdefense…

«Lois de programmation militaire» per il periodo 2014-2019

La préparation de l'avenir

Elle se traduit par les crédits accordés à la **recherche et aux études amont**, dont les montants sont sanctuarisés sur la durée de la programmation (à hauteur de 730 M€). Il se traduit également par les grands projets adaptés aux priorités de l'avenir définies dans le LBDSN. Ainsi un effort spécifique et important sera engagé dans le renseignement. La priorité sera donnée aux grands équipements faisant appel aux meilleures ressources technologiques.

Concernant la cyberdéfense, la loi de programmation militaire prend en compte cette rupture stratégique en prévoyant tout à la fois une adaptation de notre droit, un renforcement de nos capacités militaires (recrutement de plusieurs centaines de spécialistes), la mise en place d'une organisation et d'une chaîne opérationnelle centralisée, et enfin un effort important en termes d'études amont et de développement.

Priorité à l'Europe de la Défense

Les programmes d'armement en coopération européenne sont préservés. De même, de nouveaux programmes sont lancés par la loi de programmation militaire : missile antinavires léger (ANL), système de drone anti-mines futur (SLAMF).

… ma ecco che cominciano palesarsi anche altri obiettivi che vanno oltre l'esigenza di attrezzarsi per la cyberwar.

«Lois de programmation militaire» per il periodo 2014-2019

Face à l'augmentation en quantité et en sophistication des attaques informatiques, et à leurs impacts potentiellement destructeurs, l'ANSSI a pour mission d'accompagner les opérateurs d'importance vitale (OIV) dans la sécurisation de leurs systèmes d'information sensibles.

La cybersécurité des OIV s'intègre dans le dispositif interministériel plus large de sécurité des activités d'importance vitale (SAIV) inscrit dans le code de la défense. Ces activités sont réparties par secteur d'activité↗ rattaché à un ministère coordonnateur. Interlocuteur privilégié pour l'ensemble des enjeux « métier », le ministère est chargé d'apporter son expertise sur le secteur d'activité dont il a la charge.

Ce dispositif a permis d'identifier les opérateurs d'importance vitale (OIV), privés et publics, qui exploitent ou utilisent des installations jugées indispensables pour la survie de la Nation.

Pour faire face aux nouvelles menaces cyber, l'article 22 de la loi de programmation militaire↗ (loi n° 2013-1168 du 18 décembre 2013), qui fait suite aux préconisations du Livre blanc sur la défense et la sécurité nationale de 2013↗ rajoute une pierre à l'édifice en imposant aux OIV le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale (SIIV).

Cette sécurisation passe notamment par l'application d'un certain nombre de règles de sécurité. La France est le premier pays à être passé par la réglementation pour mettre en place un dispositif efficace et obligatoire de cybersécurité de ces infrastructures critiques.

ESTRATTO DA: https://www.ssi.gouv.fr/administration/protection-des-oiv/protection-des-oiv-en-france/

«Lois de programmation militaire» com'è oggi

ESTRATTO DA: https://www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits//

LPM è già stata aggiornata per il quinquennio successivo ed ora è una realtà che vincola il mercato: i soggetti coinvolti devono utilizzare prodotti «qualificati» dalle autorità.

«Lois de programmation militaire»: impatto a favore degli interessi strategici industria e servizi ICT

Liste des produits qualifiés

	Date de début de la qualification	Date de fin de la qualification	Niveau de qualification	Niveau d'agrément	Niveau de recommandation	Référence de la décision de qualification
Equipements de chiffrement IP, ethernet etc…						
Thales SIX GTS France - Gateway IPsec Mistral VS9						
VS9.0 embarqué sur les boitiers matériel IP9001	23/07/2021	01/08/2024	Standard	Diffusion Restreinte	✓	1960
Infrastructure de Gestion des clés et cartes à puce						
Austria Card - ACOS-ID v2.0 eMRTD (B) EAC/PACE configuration						
2.0 eMRTD (B)	24/06/2022	24/06/2025	Renforcé		✓	1388
Austria Card - ACOS-IDv2.0 SSCD (A) CB-Comm						
V2.0 SSCD (A)	28/07/2022	28/07/2025	Renforcé		✓	1724
Austria Card - ACOS-IDv2.0 SSCD (A) CL-TC-Comm						
V2.0 SSCD (A)	28/07/2022	28/07/2025	Renforcé		✓	1726
Bull / Groupe Atos - Trustway Proteccio						
EL/HR X163 V162	17/05/2021	15/04/2024	Renforcé	Diffusion Restreinte	✓	1219
Idemia - CombICAO Applet v2.1 on ID-one cosmo v9.1 platform en configuration SSCD						
2.1	31/07/2020	31/07/2023	Renforcé		✓	1767
Idemia - CombICAO Applet v2.1 on ID-one cosmo v9.2 platform en configuration SSCD						
2.1	31/07/2020	31/07/2023	Renforcé		✓	1768
Idemia France - CombICAO Applet v3 on ID-One Cosmo X (EAC configuration)						
Version v3.0	25/04/2022	25/04/2025	Renforcé		✓	983
Idemia France - CombICAO Applet v3 on ID-One Cosmo X (EAC with PACE configuration)						
Version v3.0	25/04/2022	25/04/2025	Renforcé		✓	980
Idemia France - CombICAO Applet v3 on ID-One Cosmo X (EAC with PACE for French ID configuration)						
Version v3.0	25/04/2022	25/04/2025	Renforcé		✓	978
Idemia France - CombICAO Applet v3 on ID-One Cosmo X (SSCD configuration)						

Page 2 sur 20

Liste des services qualifiés

	Date de début de la qualification	Date de fin de la qualification	Niveau de recommandation	Audit architecture	Audit de configuration	Audit de code Source	Tests d'intrusion	Audit organisationnel et physique	Référence de la qualification
PASSI LPM									
Advens	16/12/2021	03/09/2024	✓	×	×	×	×	×	3171
Airbus Protect	26/08/2022	01/11/2024	✓	×	×		×	×	1950
Amossys	18/02/2020	26/12/2022	✓	×	×	×	×	×	516
Atos Digital Security	25/04/2022	17/02/2023	✓	×	×	×	×	×	969
Capgemini / Sogeti ESEC	24/03/2020	26/12/2022	✓	×	×	×	×	×	914
CGI France	25/04/2022	30/09/2024	✓	×	×	×	×	×	994
Cogiceo	06/12/2021	04/11/2022	✗	×	×	×	×	×	3028
CS Novidy's	18/03/2022	01/04/2025	✓	×	×	×	×	×	608
Headmind Partners	18/03/2022	06/02/2023	✓	×	×		×	×	606

Page 7 sur 20

La qualificazione è ovviamente aperta ai player internazionali: ma nei fatti i player francesi, o quelli con filiali in Francia, risultano *de facto* avvantaggiati !

«Lois de programmation militaire» e Direttiva NIS: un'ipotesi molto probabile di cosa accadrà!

L'implementazione in Europa della Direttiva NIS troverà la Francia in posizione di preminenza rispetto agli altri partner!

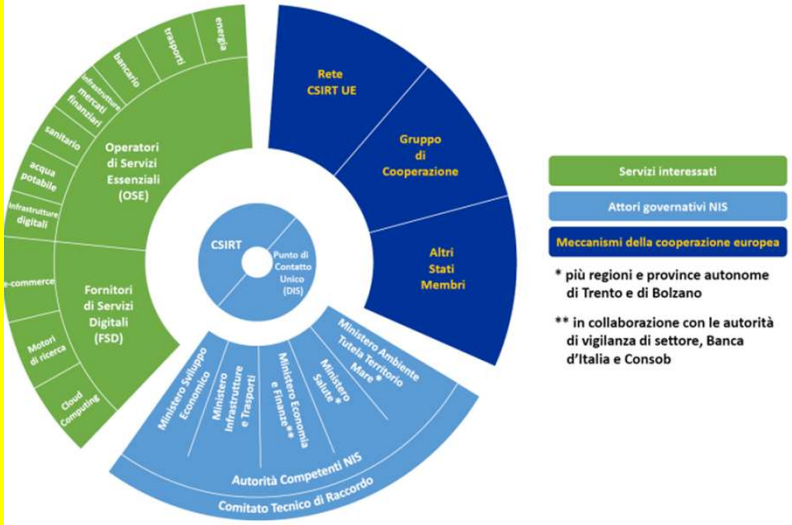
Cosa probabilmente accadrà? La riproposizione della situazione di vantaggio strategico già vista nel 1981 con l'inaugurazione del il 1° TGV.

La NIS in pillole

Con il **Decreto Legislativo 18 maggio 2018, n.65**, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018, l'Italia ha dato attuazione, recependola nell'ordinamento nazionale, alla Direttiva (UE) 2016/1148, cd. **Direttiva NIS**, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Il decreto si applica agli **Operatori di Servizi Essenziali (OSE)** e ai **Fornitori di Servizi Digitali (FSD)**.

Gli **OSE** sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori **sanitario**, dell'**energia**, dei **trasporti**, **bancario**, delle **infrastrutture dei mercati finanziari**, della **fornitura e distribuzione di acqua potabile** e delle **infrastrutture digitali**.

Gli **FSD** sono le persone giuridiche che forniscono servizi di *e-commerce*, *cloud computing* o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale. Gli obblighi previsti per gli FSD non si applicano alle **imprese** che la normativa europea definisce "**piccole**" e "**micro**", quelle cioè che hanno meno di 50 dipendenti e un fatturato o bilancio annuo non superiore ai 10 milioni di Euro.



- Tanto gli **OSE** che gli **FSD**:
  - sono chiamati ad adottare **misure tecniche e organizzative adeguate e proporzionate** alla **gestione dei rischi** e a **prevenire** e **minimizzare l'impatto degli incidenti** a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio;
  - hanno l'**obbligo di notificare**, senza **ingiustificato ritardo**, gli **incidenti** che hanno un **impatto rilevante**, rispettivamente sulla continuità e sulla fornitura del servizio, al *Computer Security Incident Response Team* (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento.

ESTRATTO DA: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/La-NIS-in-pillole.pdf

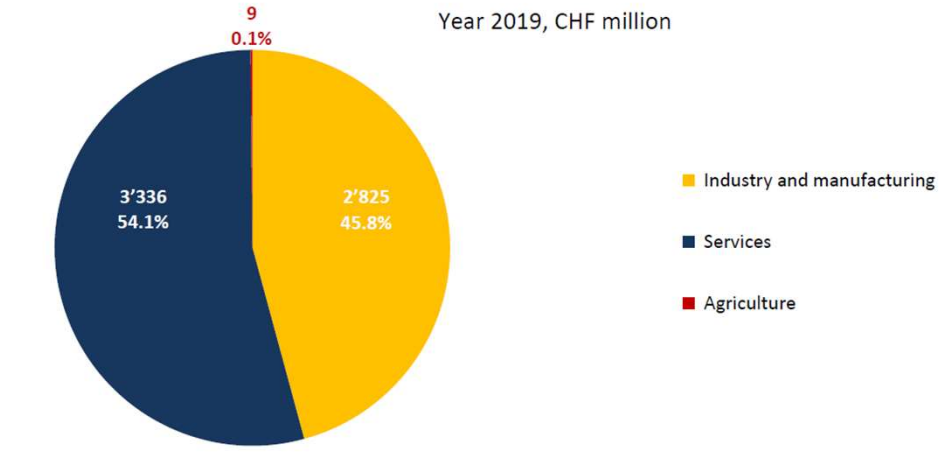
Un altro caso di interesse: il Liechtenstein

ESTRATTO DA: https://www.liechtenstein.li/en

The Principality of Liechtenstein

The Principality of Liechtenstein is located in the heart of Europe's alpine region, between Switzerland and Austria. It is home to around 38,500 inhabitants. Covering an area of 160km², it is the fourth-smallest state in Europe and the sixth-smallest in the world. Yet, despite its compact size, the Principality of Liechtenstein offers everything you could wish for: mighty mountain landscapes, a vibrant cultural scene, charming villages and plenty of opportunities for entrepreneurs.

Gross value added by economic sector



Data source: OSL (National Accounts).

ESTRATTO DA: JUN 2022, Government of the Principality of Liechtenstein, *Economic and financial data on Liechtenstein, Data as of end of June 2022.*

Un altro caso di interesse: il Liechtenstein

2020	Liechtenstein	Switzerland	Austria	Germany	Luxembourg
Gross domestic product, CHF billion	5.7	706	406	3'605	69
Population (as of 1 July)	38'896	8'654'622	9'006'398	83'783'942	625'978
Employees (annual average)	40'467	5'077'216	4'296'919	44'803'000	472'189
Full-time equivalents (annual average)	34'434	4'239'303			
GDP/capita (population), CHF	147'599	81'603	45'086	43'027	109'826
Productivity (GDP/employees), CHF	141'870	139'100	94'501	80'463	145'596
Productivity (GDP/FTE), CHF	166'725	166'594			

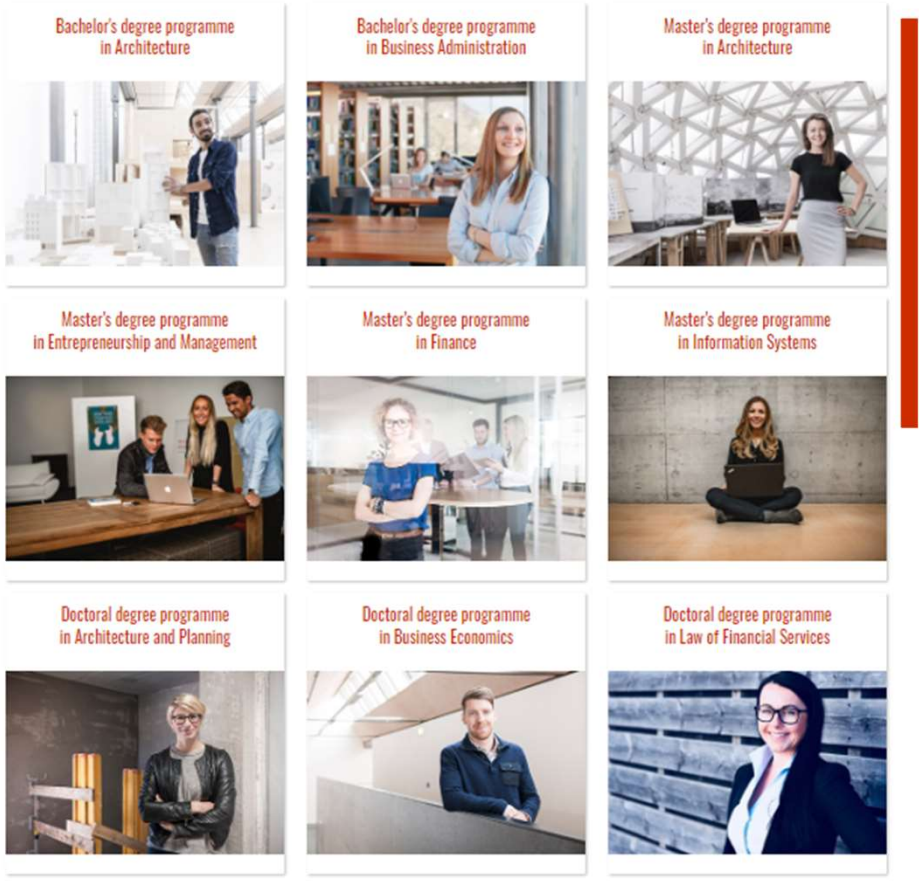
Gross value added shares (2019) by economic activity (NOGA)	Liechten-stein	Switzer-land
Agriculture, forestry, fishing (NOGA 01–03)	0.1%	0.6%
Mining and quarrying (05–09)	0.1%	0.1%
Manufacturing (10–33)	40.1%	18.7%
Electricity/water supply, sewerage, waste management and remediation activities (35–39)	1.3%	1.9%
Construction (41-43)	4.3%	4.9%
Wholesale and retail trade; repair of motor vehicles (45–47)	4.9%	15.0%
Transportation/storage (49–53)	1.7%	4.0%
Accommodation and food service activities (55–56)	0.9%	1.9%
Information/communication (58–63)	1.8%	4.5%
Financial and insurance activities (64–66)	11.5%	9.8%
Real estate activities (68)	6.5%	6.9%
Self-employed/scientific/technical support activities (69–75)	14.1%	7.6%
Other economic support activities (77-82)	1.9%	3.2%
Public administration, defence, compulsory social security (84)	6.0%	10.1%
Education (85)	0.6%	0.6%
Human health and social work activities (86–88)	2.5%	7.8%
Arts, entertainment, recreation (90–93)	0.9%	0.7%
Other service activities (94-96)	0.4%	1.3%
Activities of households as employers (97)	0.2%	0.3%

ESTRATTO DA: JUN 2022, Government of the Principality of Liechtenstein, *Economic and financial data on Liechtenstein, Data as of end of June 2022.*

Un'economia forte: industria e manifattura anche ad alta tecnologia, servizi finanziari e assicurativi

L'alta formazione nel Liechtenstein: impatto a favore degli interessi strategici del PIL nazionale

La prospettiva difensiva della cybersecurity diviene sostegno proattivo alla crescita del settore finanziario; contribuisce a diffondere la sensazione di solidità e sicurezza del settore bancario e della tutela dei patrimoni che giungono da tutto il mondo.



ESTRATTO DA: https://www.uni.li/en

La Svizzera ed i bunker che conservano informazioni

ESTRATTO DA: https://www.idealista.it/news/immobiliare/internazionale/2015/07/07/116889-falsi-chalet-sono-cosi-i-bunker-dellesercito-svizzero-nascosti-allinterno-di

Un business elvetico spesso noto solo per la sua apparente estrosità …

idealista/news

Cerchi notizie, reportage · Iscriviti · Il tuo acco

Immobiliare | Finanza | Vacanze | Deco | Aste immobiliari | Speciali | L'Opinione | Forum | Statistiche | Ricerca imm

Residenziale | Uffici | Locali commerciali | Logistica | Asset alternativi | Imprese | Costruzioni | Internazionale | Top idealista

"Falsi chalet": sono così i bunker dell'esercito svizzero nascosti all'interno di deliziose case di montagna (Fotogallery)

Commenti: 0

autorizado

Author: Redazione

7 Luglio 2015, 10:01

All'apparenza sono case idilliache, tipici chalet alpini proprio come quelli raffigurati sulle cartoline. Ma, in realtà, queste case di montagna nascondono un oscuro segreto: dietro le loro colorate facciate e le loro preziose finestre in legno si nascondono **i muri di cemento dei bunker dell'esercito svizzero.**

SWI swissinfo.ch

Prospettive svizzere in 10 lingue

AAA vendesi Bunker militare

Altri sviluppi

Vendesi Bunker

25 gen 2016 •

Ogni anno l'esercito svizzero mette in vendita una ventina di oggetti immobiliari. Questa volta è il turno del bunker di Bellegarde nel Canton Friburgo

25 gennaio 2016 - 21:58

ESTRATTO DA: https://www.swissinfo.ch/ita/aaa-vendesi-bunker-militare/42616896

La Svizzera ed i bunker che conservano informazioni

ISPI ISTITUTO PER GLI STUDI DI POLITICA INTERNAZIONALE

HOME RICERCA ISPI SCHOOL PUBBLICAZIONI EVENTI PER IMPRESE

Commentary

Datagate: la linea sottile tra sicurezza e libertà

Davide Borsani
10 giugno 2013

DOWNLOAD PDF

L'ironia della sorte ha voluto che, mentre Barack Obama accusava la Cina di Xi Jinping di condurre attacchi di spionaggio informatico nei confronti degli Stati Uniti, il britannico The Guardian e l'americano Washington Post rendessero pubblica l'attività di spionaggio condotta dalle stesse agenzie federali statunitensi, nella fattispecie la National Security Agency, nei confronti dei propri cittadini. La "talpa" dei due quotidiani, il ventinovenne Edward Snowden (già analista della NSA), ha giustificato la propria azione con la necessità di rimettere «nelle mani dei cittadini» il destino del proprio paese, altrimenti «rischiamo di diventare una tirannia».

ESTRATTO DA:
https://www.ispionline.it/it/pubblicazione/datagate-la-linea-sottile-tra-sicurezza-e-liberta-8010

… ma nel 2013 il Datagate innesca una nuova forma di business !

TOM'S HARDWARE GAME DIVISION MOBILELABS CULTURA POP MOTORLABS B2BLABS OFFERTE FORUM

Tom's Hardware vive grazie al suo pubblico. Quando compri qualcosa dai nostri link, potremmo guadagnare una commissione. Scopri di più

MANAGER

In Svizzera ex bunker militari per proteggere i dati dall'NSA

di Elena Re Garbagnati

venerdì 6 Dicembre 2013 15:52

1 min vai ai commenti

55 bunker militari dismessi alla fine della guerra fredda **sono diventati datacenter super protetti** che vengono affittati a 250mila euro al mese. Chi ne vuole comprare uno deve sborsare 15 milioni di euro. È uno degli effetti collaterali del **datagate, che ha aperto una nuova era d'oro per la Svizzera**.

ESTRATTO DA:
https://www.tomshw.it/business/in-svizzera-ex-bunker-militari-per-proteggere-i-dati-dallnsa/?amp

La Svizzera ed i bunker che conservano informazioni

ESTRATTO DA: https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20133927

L'Assemblea federale – Il Parlamento svizzero
Curia Vista – Banca dati degli atti parlamentari

13.3927 Interpellanza

Protezione dei bunker svizzeri per l'archiviazione dei dati

Depositato da: Reimann Lukas
Gruppo dell'Unione democratica di Centro
Unione democratica di Centro

Data del deposito: 27.09.2013

Depositato in: Consiglio nazionale

Stato delle deliberazioni: Liquidato

Testo depositato

In seguito alle rivelazioni di Edward Snowden in merito alle attività di spionaggio degli Stati Uniti, l'attrattiva della Svizzera quale ubicazione di server di computer è aumentata in modo significativo. Diversi esperti di sicurezza informatica mettono in guardia che con l'incremento delle informazioni conservate nei bunker del nostro Paese aumenta di conseguenza anche l'interesse dei servizi esteri stranieri per la Svizzera. Numerosi esperti si dicono sorpresi dall'ingenuità e dal disinteresse delle autorità svizzere che presto dovranno confrontarsi con questo problema.

Al riguardo il Consiglio federale è invitato a rispondere alle seguenti domande:

1. Il Consiglio federale intende provvedere affinché sia possibile contrastare tale minaccia nei confronti della Svizzera e che ciò avvenga realmente?
2. Quali misure intende intraprendere concretamente?
3. È certo che i dati acquisiti da attività di spionaggio non vengano usati da autorità svizzere, per esempio dal DFF, contro persone nel nostro Paese?
4. Per quanto concerne i danni in Svizzera risultanti dallo spionaggio estero di dati, il Consiglio federale è disposto a computarli – o ad ammetterne la computabilità e a farla valere – nel quadro di rivendicazioni estere (per es. contro banche con sede in Svizzera) provenienti da Stati all'origine di tale spionaggio?
5. È disposto a chiudere sedi e installazioni di imprese estere e svizzere ubicate nel nostro Paese qualora le loro attività servissero comprovatamente allo spionaggio di dati?

Il Consiglio federale ha naturalmente risposto al parlamentare interpellante, ma il risultato finale è stato: «**Liquidato**».

Sono stati preservati gli interessi federali in merito:

- ai ritorni economici per l'hosting dei dati, la vendita e l'affitto dei bunker
- a preservare l'immagine *di buoni custodi* di quanto si deposita in Svizzera

Le prime normazioni sistemiche di sicurezza informatica in Europa

BS 7799

- 1995, British Standards Institution (BSI)
- Emessa dal Dipartimento del Commercio ed Industria del Governo Britannico
- Contiene **best practices** per l' Information Security Management (ISM)

BS 7799 part 2

- 1999, British Standards Institution (BSI)
- É indirizzata a come implementare un Information Security Management System (ISMS)

ISO/IEC 27001

- 2005, emessa congiuntamente dall'International Organization for Standardization (ISO) e dall'International Electrotechnical Commission (IEC)
- diventa uno standard internazionale su come gestire la sicurezza delle informazioni
- non è solo uno standard di sicurezza informatica perché prende in conto: sicurezza logica + sicurezza fisica e ambientale + sicurezza organizzativa.

- Si giunge a gestire la qualità: controlli di qualità, sistemi di gestione, …
- Deriva da un approccio originario che ha nel business dell'organizzazione l'obiettivo finale: va garantito il corretto e adeguato funzionamento dei processi aziendali e dei sistemi informatici utilizzati.

L’approccio inizialmente adottato nella normazione italiana

Legge 675 del 1996

- Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali

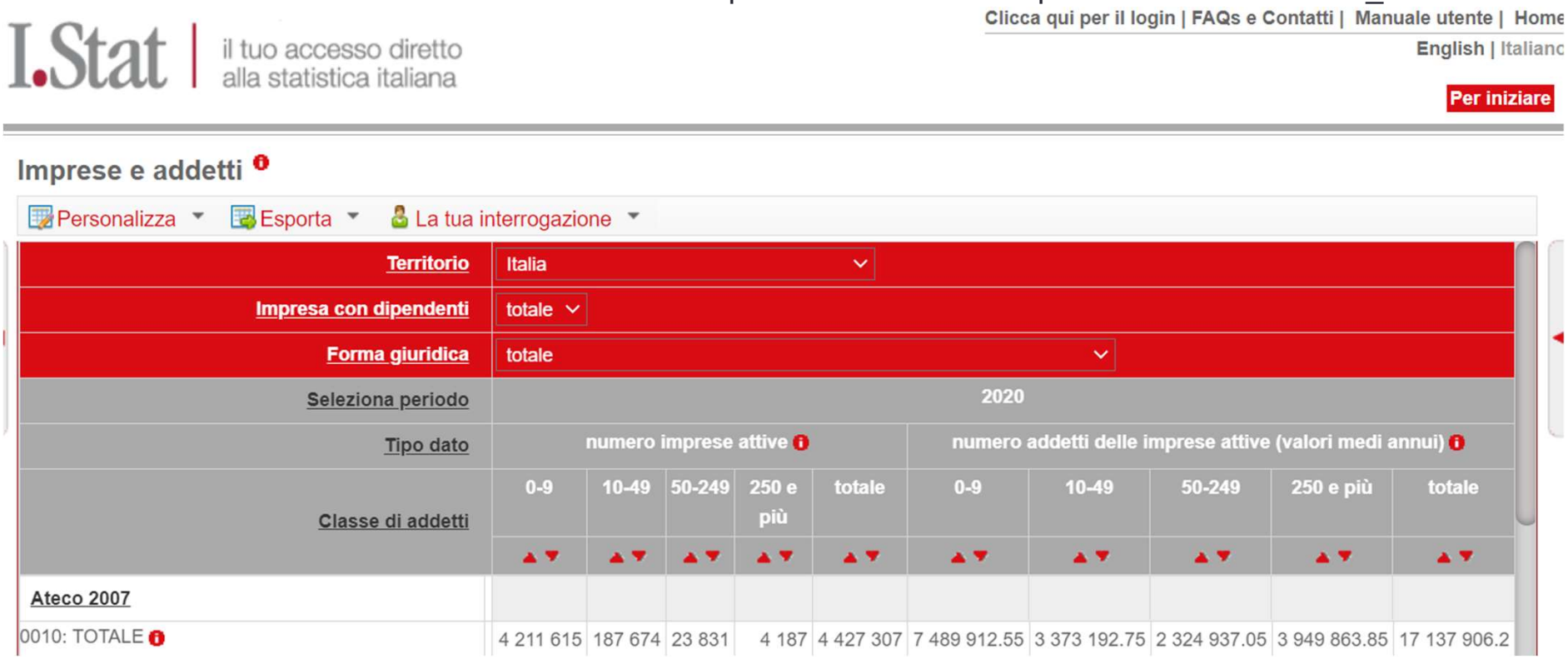
Codice della privacy

- Decreto Legislativo 30 giugno 2003, n.196, recante il “Codice in materia di protezione dei dati personali”
- Implementa la Direttiva 95/46/CE: armonizzazione delle norme in materia di protezione dei dati personali per garantire un flusso libero dei dati promuovendo al contempo un elevato livello di tutela dei diritti fondamentali dei cittadini.
- Introduce l’Allegato B: Disciplinare tecnico in materia di misure minime di sicurezza

Approccio originario di tipo giuridico: tutela dei diritti individuali in un contesto di norme armonizzate all’interno di un mercato/spazio economico comune europeo.

Le prime normazioni sistemiche di sicurezza informatica in Europa: rischio di impatto nel paese Italia

ESTRATTO DA: http://dati.istat.it/Index.aspx?DataSetCode=DICA_ASIAUE1P



I.Stat | il tuo accesso diretto alla statistica italiana

Clicca qui per il login | FAQs e Contatti | Manuale utente | Home

English | Italianc

Per iniziare

Imprese e addetti

Personalizza | Esporta | La tua interrogazione

Territorio	Italia								
Impresa con dipendenti	totale								
Forma giuridica	totale								
Seleziona periodo	2020								
Tipo dato	numero imprese attive					numero addetti delle imprese attive (valori medi annui)			
Classe di addetti	0-9	10-49	50-249	250 e più	totale	0-9	10-49	50-249	250 e più	totale
Ateco 2007										
0010: TOTALE	4 211 615	187 674	23 831	4 187	4 427 307	7 489 912.55	3 373 192.75	2 324 937.05	3 949 863.85	17 137 906.2

$$\frac{17.137.906{,}20}{4.427.307{,}00} = 3{,}87 \text{ dipendenti medi per azienda}$$

Questi sono dati più recenti, ma poco cambia: la dimensione media dell'azienda italiana avrebbe difficilmente supportato l'impatto iniziale di norme pensate per contesti generalmente più strutturati.

L'Italia e l'approccio prescrittivo a tutela dell'interesse delle proprie PMI

ALLEGATO B. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA - D.LGS. 196/03
(Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

L'approccio prescrittivo ha semplificato gli obblighi a carico delle PMI italiane.

È stato preservato l'interesse nazionale connesso all'operatività delle piccole aziende: dove non è generalmente diffuso il know-how dei sistemi di gestione e qualità.

GDPR: il nuovo approccio europeo alla normazione ed i suoi riflessi nella cybersecurity

ESTRATTO DA: https://www.garanteprivacy.it/regolamentoue

Avevamo già discusso (e previsto) nel 2013 i vantaggi strategici di un quadro normativo omogeneo

ESTRATTO DA: Muzzì C., Big Data: limitazioni e opportunità geopolitiche e geoeconomiche, Atti del 50° Congresso Nazionale AICA, 2013

Big Data: limitazioni e opportunità geopolitiche e geoeconomiche

Carlo Muzzì
AICA - Associazione Italiana per l'Informatica ed il Calcolo Automatico
muzzi@acm.org

Abstract. *The idea that Bi*
frontier for innovation, comp
global economy is now ger
many geo-political and g
influence them in the global c
analyzed in this study, along

Keywords: Big Data, conditions, oppo

1. Introduzione

L'idea che i Big Data possan
l'innovazione, la competizione e la pr
et al, 2011] è oramai generalmente
inizialmente circoscritto alla letteratura
anche nella più generale comunicazio
(eseguita l'8 giugno 2013) dell'occorre
ha restituito circa 1.870.000.000 voci,
ore. Anche se l'ambito di applicazione
estremamente vario e distribuito, sc
come alcune condizioni geopolitiche
scenario planetario lo influenzeranno f
sulle possibilità di costituire realmente
per uscire dalla crisi economica ancora in atto.

[Mantelero, 2012]. Anche il contesto giuridico può dunque spingere gli attori di questo settore a trasferire o implementare i propri sistemi (data center, cloud computer, ecc.) nelle nazioni ritenute più favorevoli. Non essendo questo il luogo deputato a trattare di cyber crime escludiamo dalla nostra analisi approfondimenti su quelle nazioni che, per minor sviluppo o per qualche forma di complicità, dispongono addirittura di un quadro legislativo favorevole verso talune azioni illecite; rivolgiamo invece la nostra attenzione sulla chiarezza del quadro normativo: emerge che negli USA, al vantaggio della preminenza del settore dell'ICT, si aggiunge la leva competitiva di una normativa più armoniosa rispetto a quella ad esempio esistente nei diversi stati dell'Unione Europea [Mantelero, 2012]. La recente proposta della Commissione europea per un nuovo regolamento continentale che costituisca una quadro giuridico omogeneo in materia di protezione dei dati, potrebbe, se approvata, fornire maggiore competitività anche ai player europei [Commissione europea, 2013].

GDPR: nuova approccio alla sicurezza

responsabilizzazione o accountability

- adozione di comportamenti proattivi che dimostrino l'adozione concreta di misure che hanno l'obiettivo di assicurare l'applicazione del regolamento

data protection by default and by design

- progettare anche la sicurezza prima di trattare
- analisi preventiva e impegno applicativo dei titolari mediante l'esecuzione di attività specifiche e dimostrabili
- configurare a monte per ridurre i rischi

rischio inerente al trattamento

- analisi e valutazione dei rischi
- DPIA

Intervento delle autorità di controllo sostanzialmente «ex post»: dopo le autonome determinazioni dei titolari

- Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio»
- Non ci sono misure minime ma idonee

Interessi raggiunti:

- maggiori quote di mercato per la cybersecurity
- la R&D di nuovi prodotti e e servizi incorpora (o in taluni casi può avvenire) solo grazie all'R&D in cybersecurity

GDPR e interessi strategici raggiunti dall'Europa

Microsoft: due nuovi datacenter cloud in Germania che opereranno sotto le leggi tedesche

Annuncio importante dall'azienda di Redmond: due nuovi datacenter cloud saranno aperti in territorio tedesco e opereranno, grazie alla gestione da parte di una società tedesca, secondo le leggi locali. Microsoft non potrà, pertanto, accedere ai dati degli utenti

di Andrea Bai pubblicata il **14 Novembre 2015**, alle **10:31** nel canale PRIVATE CLOUD

Microsoft | Azure

Grandi novità per il cloud di **Microsoft**: la società statunitense ha infatti annunciato l'imminente apertura di due nuovi datacenter in Germania che saranno gestiti da una terza parte che fungerà da "amministratore fiduciario" e che opererà secondo la normativa tedesca. Ciò significa che Microsoft non potrà accedere ai dati degli utenti senza il permesso di questo amministratore o del proprietario dei dati, anche se intimata dalle autorità USA. E, anche nel caso in cui Microsoft ottenga l'autorizzazione da parte dell'amministratore, l'accesso ai dati avverrà solamente sotto la supervisione di quest'ultimo.

ESTRATTO DA: https://edge9.hwupgrade.it/news/private-cloud/microsoft-due-nuovi-datacenter-cloud-in-germania-che-opereranno-sotto-le-leggi-tedesche_59575.html

Già prima dell'entrata in vigore del GDPR (ed anche per rispondere al Datagate) la Germania diviene sede di 2 nuovi Data Center Microsoft.

Interessi strategici promossi per cybersecurity ed altro:

- sicurezza nazionale
- aumento del PIL
- tutela della propria cittadinanza digitale

GDPR e interessi strategici raggiunti dall'Europa

Posizioni dei dati per l'Unione europea

Articolo • 25/10/2022 • 10 minuti per la lettura • 8 contributori

Commenti e suggerimenti

I dati dei clienti sono fondamentali

Microsoft riconosce l'importanza di mantenere la privacy e la riservatezza dei dati aziendali. I dati appartengono all'utente, che può accedervi, modificarli o eliminarli in qualsiasi momento. Microsoft non userà i dati senza il consenso dell'utente e, dopo il consenso, userà i dati solo per fornire i servizi che si sono scelti. Se l'utente lascia uno dei servizi, si garantisce la conservazione dei dati personali da parte dell'utente attraverso la rimozione dei dati dai sistemi secondo rigorosi standard e processi.

Dove vengono archiviati i dati UE dei clienti

Il data center GEOS è disponibile in Germania e in Francia e consente di archiviare i dati nel proprio paese, se ivi è ubicata l'azienda. I data center dell'Unione europea si trovano in Austria, Finlandia, Francia, Irlanda e Paesi Bassi. I dati dei servizi seguenti verranno ospitati nelle posizioni seguenti in base all'indirizzo di fatturazione scelto:

Nome del servizio	Posizione dei tenant creati con un indirizzo di fatturazione in Francia	Posizione dei tenant creati con un indirizzo di fatturazione in Germania	Posizione per i tenant creati con un indirizzo di fatturazione in altri paesi UE
Exchange Online	Francia	Germania	Unione Europea
OneDrive for Business	Francia	Germania	Unione Europea
SharePoint Online	Francia	Germania	Unione Europea
Skype for Business	Unione Europea	Unione Europea	Unione Europea
Microsoft Teams	Francia	Germania	Unione Europea
Office Online & Mobile	Francia	Germania	Unione Europea
Exchange Online Protection	Francia	Germania	Unione Europea
Intune	Unione Europea	Unione Europea	Unione Europea
MyAnalytics	Francia	Germania	Unione Europea
Planner	Unione Europea	Unione Europea	Unione Europea

Microsoft oggi commercializza soluzioni cloud per gli europei in Data Center europei

Interessi strategici promossi per cybersecurity ed altro:

- ...quelli già citati +
- Europa attrattiva e competitiva sul mercato globale del cloud commerciali

ESTRATTO DA: https://learn.microsoft.com/it-it/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide

GDPR e interessi strategici raggiunti dall'Europa

ESTRATTO DA: https://blog.google/intl/it-it/prodotti/cloud/le-google-cloud-region-di-milano-e-torino-generano-un-nuovo-mercato-per-i-partner-del-valore-di-19-miliardi-di-euro/

GOOGLE CLOUD

Le Google Cloud region di Milano e Torino generano un nuovo mercato per i partner del valore di 1.9 miliardi di Euro

Accenture, Bip, Capgemini, Deloitte, Huware, Injenia, NTT DATA, Reply, SAP e TIM tra i partner chiave di Google Cloud che supportano la trasformazione digitale del Paese, facendo leva sulle nuove region italiane.

22 Lug, 2022 · 5 minuti di lettura

F **Fabio Fregi**
Country Manager Italy, Google Cloud

Anche Google ha aperto 2 cloud regions in Italia: un unicum !

Interessi strategici promossi per cybersecurity ed altro:

- ...quelli già citati +
- supporto alla trasformazione digitale dell'Italia (recupero del gap)
- promozione della ricerca e delle start-up

GDPR: un modello di riferimento nel mondo

Cos'è PIPEDA?

PIPEDA è l'abbreviazione di ***Personal Information Protection and Electronic Documents Act*** e fa riferimento al nuovo regolamento generale canadese sulla protezione dei dati. L'emendamento combina le due precedenti leggi canadesi sulla protezione ***dei dati Consumer Privacy Protection Act*** **(CPPA)** e ***Personal Information and Data Protection Tribunal Act (PIDPTA)*** in un regolamento completo equivalente al GDPR. Il riferimento al regolamento generale europeo sulla protezione dei dati può essere visto in molti punti di PIPEDA, motivo per cui viene spesso chiamato anche GDPR Canada.

ESTRATTO DA:
https://www.consentmanager.it/conoscenza/destra/pipeda-il-regolamento-generale-canadese-sulla-protezione-dei-dati/

ESTRATTO DA:
https://www.riskmanagement360.it/compliance/nuova-legge-svizzera-sulla-protezione-dei-dati-e-gdpr-un-confronto-operativo-per-le-imprese/

NETWORK DIGITAL 360 I NOSTRI SERVI

RISK MANAGEMENT 360

NORMATIVE INTERNAZIONALI

Nuova legge svizzera sulla protezione dei dati e GDPR, un confronto operativo per le imprese

Home › Compliance

Condividi questo articolo

La nuova legge federale sulla protezione dei dati (LPD) della Confederazione Svizzera è stata adottata il 25 settembre 2020 ed entrerà in vigore il 1° gennaio 2022. In parte recepisce i dettami del GDPR, ma ci sono delle differenze. Le regole per le società italo-svizzere.

ESTRATTO DA:
https://www.corrierecomunicazioni.it/privacy/privacy-in-india-tutto-da-rifare-il-piano-non-convince-il-governo/

Privacy, in India tutto da rifare: il piano non convince il Governo

Home › Privacy

Condividi questo articolo

Stralciata la nuova proposta di legge sui dati personali che aveva suscitato proteste da parte delle big tech e non solo. Ma si rischia l'effetto boomerang: la revisione potrebbe sortire maggiori poteri per lo Stato sulla base di un modello più vicino a quello cinese che a quello europeo

11 Ago 2022

Israele: (un) il caso di successo

How Israel became the world's cyber powerhouse

Smart decisions and a need for protection have made Israel the world's cyber leader, with 40% of all cyber investments made in the country. A new book charts the rise and rise.

By Abigail Klein Leichman | NOVEMBER 29, 2021, 12:40 PM

It is not by chance that 40 percent of all private cyber investments in the world are invested in Israeli companies, and that a third of the world's unicorn cyber companies – private startups worth at least $1 billion – are Israeli.

ESTRATTO DA: https://www.israel21c.org/how-israel-became-the-worlds-cyber-powerhouse/

Interessi strategici promossi per cybersecurity ed altro:

- ...quelli già citati +
- supporto alla politica nazionale ed internazionale dello stato

Una sintesi di quanto abbiamo già discusso su come diventare un leader nella cybersecurity

GOVINSIDER

How Israel became a global cybersecurity powerhouse

Doron Tamir, Founder of Israeli National Cyber Directorate, shares the secrets behind Israe. success in the cybersecurity sector.

By Liew Ming En

25 NOV 2021

DATA

1. Invest in cybersecurity education
2. Learn from the financial sector
3. Be forward thinking and creative

ESTRATTO DA: https://govinsider.asia/data/how-israel-became-a-global-cybersecurity-powerhouse-doron-tamir/

La Cina: un altro modo di tutelare la propria sovranità digitale e promuovere il proprio sviluppo tecnologico-industriale

ESTRATTO DA: https://eastwest.eu/it/cina-al-bando-pc-software-americani/

ASIA CINA LA NOTIZIA DEL GIORNO

Cina, al bando pc e software stranieri

La decisione di sostituire i computer americani con dispositivi di produzione domestica entro due anni si spiega con la volontà cinese di rendersi autonoma dalle tecnologie occidentali

di **Marco Dell'Aguzzo** 8 Maggio 2022

Share

Interessi strategici promossi per cybersecurity ed altro:

- … quelli già citati +
- leva per il controllo interno dello stato

CHINA BRIEFING
From Dezan Shira & Associates

TOPICS > Il Mercato Cinese Del Cloud Computing: Sviluppi E Opportunità Per Gli Operatori Stranieri

Quadro normativo e requisiti di conformità per le aziende cloud in Cina

Da quando, nel 2010, ha identificato il cloud computing come un settore emergente critico, il governo cinese ha investito e sostenuto strategicamente la crescita del cloud computing in Cina. Quando il Consiglio di Stato ha pubblicato gli obiettivi del 12° Piano quinquennale (12° FYP) (dal 2011 al 2015) per promuovere il cloud computing, i principali dipartimenti governativi hanno risposto con proposte dettagliate su come soddisfare i requisiti. I governi provinciali e locali, gli istituti di ricerca, le aziende, i laboratori di ricerca e le organizzazioni di supporto hanno a loro volta elaborato i propri piani di sviluppo in linea con gli interessi del governo centrale.

ESTRATTO DA: https://www.china-briefing.com/news/il-mercato-cinese-del-cloud-computing-sviluppi-e-opportunita-per-gli-operatori-stranieri/

USA: la cybersecurity come una delle leve per mantenere la propria leadership politica-economica-militare sul mondo

NETWORK DIGITAL 360

MENU Agenda Digitale Cittadinanza digitale Sicurezza Informatica Sanità digitale Industry

L'APPROFONDIMENTO

Cybersecurity, America is back? La nuova politica Usa, dagli slogan ai fatti

Home > Sicurezza Digitale

La nuova politica estera Usa mira rilanciare il ruolo americano nella cybersecurity e cyber diplomacy globale, agendo da "modello" agli occhi del mondo. Un piano che deve però ancora fare i conti con la realtà della società e della politica interna. Una bella sfida

14 Set 2021

La visione della cybersecurity diviene olistica.

Interessi strategici che si vogliono tutelare si espandono:

- tutela del proprio sistema democratico
- promozione della leadership militare, economica e politica!

ESTRATTO DA:
https://www.agendadigitale.eu/sicurezza/cybersecurity-america-is-back-la-nuova-politica-usa-dagli-slogan-ai-fatti/

La nuova politica estera di cybersecurity e cyber diplomacy

La nuova politica estera statunitense in ambito di cybersecurity non è più mirata principalmente a favorire un'espansione della democrazia nel mondo e a proteggere un internet "open, free, interoperable, secure, and reliable", secondo l'ideologia dominante alcuni anni fa, esemplificata nell' "International Strategy for Cyberspace" dell'amministrazione Obama nel 2011, ma vuole difendere il cyberspace da una serie di minacce, che spaziano dagli attacchi alle infrastrutture critiche e ai servizi essenziali — ormai interamente dipendenti da sistemi digitali vulnerabili — alle interferenze in elezioni nazionali, alla disinformazione, all'autoritarismo digitale di paesi autocratici.