https://en.wikipedia.org/wiki/Cyber_Essentials

Elementi essenziali per la sicurezza informatica

Da Wikipedia, l'enciclopedia libera

Cyber Essentials è uno schema di certificazione del Regno Unito progettato per dimostrare che un'organizzazione ha un livello minimo di protezione nella sicurezza informatica attraverso valutazioni annuali per mantenere la certificazione.

Sostenuto dal governo britannico e supervisionato dal **National Cyber Security Centre (NCSC).** Incoraggia le organizzazioni ad adottare buone pratiche in materia di sicurezza delle informazioni. [1] Cyber Essentials include anche un framework di garanzia e un semplice set di controlli di sicurezza per proteggere le informazioni dalle minacce provenienti da Internet.

La certificazione subirà modifiche sostanziali da gennaio 2022, tra cui l'inserimento di tutti i servizi cloud nell'ambito e una nuova sezione sull'autenticazione a più fattori insieme a modifiche su password e pin. [2]

Certificazione [modifica]

Il programma Cyber Essentials prevede due livelli, il primo è l'autocertificazione e il secondo richiede la convalida indipendente delle affermazioni fatte:[][3][4]

Cyber Essentials [modifica]

Comunemente indicato come segna i tuoi compiti a casa,[5] le organizzazioni autovalutano i loro sistemi e quindi completano una valutazione online. La valutazione online è contrassegnata da un valutatore Cyber Essentials che fornisce feedback su eventuali aree in cui potrebbero essere apportati miglioramenti.

Non esiste una convalida indipendente dell'accuratezza delle risposte a questo livello.

Il costo per Cyber Essentials parte da £ 300 ed è soggetto a IVA nel Regno Unito. Il modello di prezzo è suddiviso in livelli in base al numero di dipendenti e ulteriori informazioni sono disponibili sul sito Web IASME.

Cyber Essentials Plus [modifica]

Lo stesso del base, ma con convalida indipendente da parte di una terza parte accreditata.

I sistemi sono testati in modo indipendente e Cyber Essentials è integrato nella gestione del rischio informativo dell'organizzazione.

Il costo per l'accreditamento Plus dipende dalla complessità dell'ambiente, ma per una semplice PMI costerebbe in genere circa £ 1.400 e sarebbe soggetto a IVA nel Regno Unito. [6]

IASME ha incorporato Cyber Essentials nel più ampio standard di garanzia delle informazioni IASME. [7]

Come per ISO/IEC 27001, le organizzazioni possono scegliere di limitare l'ambito della certificazione a un determinato sottoinsieme della loro attività e questo deve essere indicato sul loro certificato.

Controlli [modifica]

I cinque controlli tecnici sono:

1. Firewall di confine e gateway Internet
2. Configurazione sicura
3. Controllo di accesso
4. Protezione da malware
5. Gestione delle patch

La guida di Cyber Essentials li suddivide in dettagli più fini.

Questi controlli possono essere mappati rispetto ai controlli richiesti da ISO/IEC 27001, lo Standard of Good Practice for Information Security e la IASME Governance,[8] sebbene Cyber Essentials abbia un focus più ristretto, enfatizzando i controlli tecnici piuttosto che la governance, il rischio e la politica.

Storia [modifica]

Il programma Cyber Essentials è stato lanciato il 5 giugno 2014. Diverse organizzazioni sono state rapidamente certificate entro la fine di giugno. [9] Da ottobre 2014, la certificazione **Cyber Essentials è richiesta per i fornitori del governo centrale del Regno Unito che gestiscono determinati tipi di informazioni sensibili e personali.** [10] L'obiettivo è incoraggiare l'adozione da parte delle imprese che desiderano presentare offerte per appalti pubblici. [11] Gli assicuratori hanno suggerito che gli organismi certificati possono attirare **premi assicurativi più bassi.** [12] Oltre 30 000 certificati Cyber Essentials sono stati assegnati ad aziende e organizzazioni. [13]

È stato sviluppato in collaborazione con partner industriali, tra cui l'Information Security Forum (ISF), l'Information Assurance for Small and Medium Enterprises Consortium (IASME) e il British Standards Institution (BSI), ed è approvato dal governo del Regno Unito. [14] È stato lanciato nel 2014 dal Dipartimento per le imprese, l'innovazione e le competenze. [15]

Dopo l'attacco ransomware WannaCry, NHS Digital ha rifiutato di finanziare 1 miliardo di sterline, che era il costo stimato per soddisfare lo standard Cyber Essentials Plus, affermando che ciò non avrebbe costituito un buon rapporto qualità-prezzo e che aveva investito oltre 60 milioni di sterline e pianificato di spendere altri 150 milioni di sterline per affrontare i principali punti deboli della sicurezza informatica nei prossimi due anni. [16]

A partire da settembre 2019, c'erano cinque organismi di accreditamento tra cui APMG, CREST, IASME, IRM security e QG. [17]

A partire da aprile 2020, IASME è stato scelto dal National Cyber Security Centre (NCSC) per essere l'unico organismo di accreditamento del Cyber Essentials Scheme.

Nel gennaio 2022 il modello di prezzo passerà a un modello a più livelli basato sul numero di dipendenti, questo per riflettere meglio la natura più complessa della valutazione delle organizzazioni più grandi. [18] I servizi cloud, BYOD, il lavoro da casa, i thin client e l'AMF vedranno grandi cambiamenti come parte della valutazione. [19]

Vedi anche [modifica]

- CESG
- Servizio digitale governativo
- Politica di classificazione della sicurezza governativa
- IASME
- ISO/IEC 27001
- NCSC
- Comunità di sicurezza informatica del Regno Unito
- Forum sulla sicurezza informatica del Regno Unito

Riferimenti[modifica]

1. ^ *"Lo schema governativo mostra di chi ci si può fidare della sicurezza informatica". Telegrafo. 5 giugno 2014. URL consultato il 1º luglio 2014*
2. ^ *"Cyber Essentials: Requisiti per l'infrastruttura IT Versione 3.0" (PDF). Centro nazionale per la sicurezza informatica. 29 novembre 2021. URL consultato il 26 dicembre 2021.*
3. ^ *"Cyber Essentials Scheme Assurance Framework" (PDF). Governo di Sua Maestà. URL consultato il 1º luglio 2014*
4. ^ *Stevevi. "UK Cyber Essentials Plus - Azure Compliance". docs.microsoft.com. URL consultato il 2021-08-20.*
5. ^ *Raywood, Dan (2017-11-17). "Cyber Essentials: Fad or Future". Rivista Infosecurity. URL consultato l'2021-02-08.*
6. ^ *"Domande frequenti - Iasme". iasme.co.uk. URL consultato l'2021-02-08.*
7. ^ *"Cyber Essentials Scheme – IASME". www.iasme.co.uk. URL consultato il 2016-09-07.*
8. ^ *"Requisiti per la protezione tecnica di base dagli attacchi informatici" (PDF). Governo di Sua Maestà. URL consultato il 1º luglio 2014*
9. ^ *"Le prime sette PMI mordono il programma Cyber Essentials di punta del governo". Mondo informatico. 30 giugno 2014. URL consultato il 1º luglio 2014*
10. ^ *"Cyber essentials scheme: panoramica". GOV.UK. URL consultato il 1º luglio 2014*
11. ^ *"Cyber risk and the UK's Cyber Essentials Scheme" (Il rischio informatico e il programma Cyber Essentials del Regno Unito). Computer settimanale. Giugno 2014. URL consultato il 1º luglio 2014*
12. ^ *"Il governo lancia lo schema di sicurezza Cyber Essentials". 6 giugno 2014. URL consultato il 1º luglio 2014*
13. ^ *"Matt Hancock's Cyber Security Speech". URL consultato il 7 luglio 2017*
14. ^ *"Cyber Essentials Scheme" (PDF). Governo di Sua Maestà. URL consultato il 9 settembre 2016*
15. ^ *"Lancio del programma 'Cyber Essentials'". ICO. URL consultato il 1º luglio 2014*
16. ^ *"I capi della sanità si rifiutano di pagare un conto da 1 miliardo di sterline per migliorare la sicurezza informatica del NHS". Costruire un'assistenza sanitaria migliore. 15 ottobre 2018. URL consultato il 27 novembre 2018*
17. ^ *"Cyber Essentials - SITO UFFICIALE". www.cyberaware.gov.uk. URL consultato il 2017-03-01.*
18. ^ *"Cyber Essentials adotterà una struttura dei prezzi a più livelli dal 2022". www.ncsc.gov.uk. URL consultato il 2021-12-18.*
19. ^ *Muncaster, Phil (2021-11-30). "Cyber Essentials pronti per grandi cambiamenti nel 2022". Rivista Infosecurity. URL consultato il 2021-12-18.*

Collegamenti esterni [modifica]

- Sito ufficiale Cyber Essentials
- Consigli ufficiali Cyber Essentials
- Guida ufficiale Cyber Essentials - Tutti gli argomenti
- Centro nazionale per la sicurezza informatica: 10 passaggi per la sicurezza informatica

Categorie:

- Organizzazioni di sicurezza informatica
- Criminalità informatica nel Regno Unito
- Standard di garanzia delle informazioni
- Governance delle informazioni
- Organizzazioni di tecnologia dell'informazione con sede nel Regno Unito