AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2022	N. 9/ 2022	Ottobre 2022

Le Pmi e la sicurezza in Rete*

La legge 133/2019 sul Perimetro di sicurezza nazionale cibernetica (Psnc) ha stilato una lista di aziende identificate come Osf, Operatori di servizi fondamentali, interessate da adempimenti per quelle aree e tecnologie sottese ai servizi interni al Perimetro stesso. È evidente che alcune Pmi sono parte della lista, tuttavia la ricaduta principale non è legata tanto alla diretta appartenenza a tale categoria, ma soprattutto alla supply chain. La norma impone infatti una serie di adempimenti che non possono essere rispettati se non si impone anche alla supply chain un comportamento sicuro.
Tutti gli appartenenti alla lista del Psnc stanno già lavorando per stringere contratti con i fornitori critici, più attenti ai requisiti di sicurezza. Molti di questi fornitori critici sono Pmi che risultano quindi molto interessate da quanto previsto dalle norme, seppur indirettamente e con un ritardo temporale. Ci aspettiamo, quindi, che le Pmi diventino più attente alla cybersecurity come risultato diretto o indiretto dell'applicazione del Psnc. Questa maggiore attenzione dovrà necessariamente comportare alcuni investimenti in sicurezza rispetto ai quali il mercato delle Pmi non sembra avere chiarezza e, tanto meno, determinazione. Lo scenario descritto evidenzia come queste aziende si trovino di fronte a nuove sfide legate alla costante evoluzione del ruolo ricoperto dalla dimensione cibernetica.
L'analisi del panorama normativo europeo e nazionale mette in luce il recente interesse delle istituzioni governative verso il tema della sicurezza informatica, considerata ormai elemento fondamentale per il funzionamento del sistema-Paese e dell'Unione europea.
Dal punto di vista nazionale i recenti sforzi per concretizzare il Perimetro di sicurezza nazionale cibernetica e istituire l'Agenzia per la cybersicurezza nazionale (Acn) si configurano come pietre miliari della nuova architettura nazionale di sicurezza cibernetica, volte a garantire presidi adeguati alle nuove sfide. Tuttavia, la concreta applicazione di quanto previsto dall'apparato normativo sinora costruito, nelle realtà di piccola e media dimensione, resta una sfida aperta. A tale complessità si aggiungono le esigue risorse impiegate da queste realtà per formare il personale e inserire risorse qualificate. Con questi presupposti non è da escludere che possano comparire forme estorsive con logiche simili al "pizzo" della criminalità organizzata traslate nella dimensione cyber. Tale fenomeno potrebbe configurare scenari molto critici per le Pmi.
Vogliamo ripristinare un'autonomia nazionale in tema digitale. L'autonomia hard implica una capacità autonoma di produzione che copra tutto il flusso della catena del valore, comprese materie prime e logistica, così come le fonderie dei microchip, e non può che essere contestualizzata a livello regionale europeo. L'autonomia digitale soft è invece nazionale, italiana e riguarda le professionalità. Purtroppo, però, le grandi aziende giocano al rialzo continuo degli stipendi, di fatto "rubandosi" l'un l'altra gli esperti in un fenomeno che abbiamo definito di "mecenatismo". Questa dinamica impedisce però a tutte le Pmi di poter assumere personale con competenze cibernetiche. Se non iniziamo a produrre cervelli, anche mediocri, in tema di cyber-security, questa disciplina resterà un privilegio di pochi.
.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

* AirPress, n.136, settembre 2022

Luisa Franchina
presidente dell'Associazione italiana esperti in infrastrutture critiche

ATTIVITA' DELL'ASSOCIAZIONE

ATTIVITA' DI EDUCATION

Sono in corso di programmazione le attività di formazione per soci e simpatizzanti che si svolgeranno nella seconda parte dell'anno 2022.

Anzitutto, l'accordo con IsacaRoma consentirà ai soci AIIC di partecipare ai loro seminari (svolti principalmente in modalità webinar) su cybersecurity, risk management e protezione dei dati.

Stiamo valutando le modalità di svolgimento di questi eventi, possibilmente – se le condizioni pandemiche lo consentiranno – in modalità mista, presenza e distanza.
Inoltre, stiamo già prendendo accordi per una ripresa delle visite aziendali presso enti/imprese di rilevanza nazionale.
Vi terremo informati.
Vi ricordiamo anche che proprio per fornire un valore aggiunto ai nostri associati, alcuni eventi saranno riservati soltanto a chi è in regola con il pagamento delle quote associative.

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.
La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

AIIC ha sottoscritto convenzioni di collaborazione con altre Associazioni. In particolare con:

- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Association for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
usare la loro esperienza comune per aiutare l'implementazione di aspetti critici del concetto di infrastruttura nell'ambito dell'UE e del quadro giuridico nazionale,
costruire e promuovere una rete europea di organizzazioni professionali ed esperti che lavorino nel campo dei servizi e della protezione delle infrastrutture critiche.
- **CENTRO RICERCHE THEMIS** – la convenzione tra AIIC e THEMIS è stata firmata il 21 marzo 2016. Le due Associazioni si sono impegnate a collaborare per la realizzazione congiunta di iniziative e servizi da proporre agli associati, secondo forme e modalità da stabilire con appositi accordi.
- **EUCONCIP** – AIIC è membro fondatore di EUCONCIP (European Cooperation Network on Critical Infractructures Protection) assieme a Fondazione Formit, ARPIC (Romanian Asociation for Critical Infrastructures and Services Protection), CCI (Centro de Ciberseguridad Industrial), CESS (Centre for European Security Strategies), S21Sec. EUCONCIP è un'associazione con sede legale in Italia, costituita nel 2016 con lo scopo di promuovere la cooperazione tra paesi e tra settori nel campo della protezione delle infrastrutture critiche. L'obiettivo principale di EUCONCIP è contribuire allo sviluppo di un approccio armonizzato da adottare per la protezione delle infrastrutture critiche che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale delle persone (Direttiva UE 2008/114 / CE).
- **AFCEA ROMA** - la convenzione tra AIIC e AFCEA – Armed Forces Communications & Electronics Association – Capitolo di Roma è stata firmata il 18 settembre 2017. Scopo della convenzione è di promuovere principi e tecniche professionali reciproche e di interesse per entrambe le Associazioni, avvicinando così le due community nazionali su tematiche comuni. La collaborazione permetterà di dare evidenza a eventi organizzati da ciascuna associazione, attraverso i propri canali di comunicazione, e di sviluppare e sostenere iniziative congiunte su temi di comune interesse.
- **AIAS** – la convenzione tra AIIC e AIAS Associazione professionale Italiana Ambiente e Sicurezza) è stata firmata il 15 febbraio 2016 con durata triennale. Le due associazioni intendono promuovere forme di collaborazione tra le attività di AIAS e delle sue società appartenenti al Networkaias e precisamente AIAS Academy e di AIASCert e le attività di AIIC al fine di promuovere una cultura applicativa di una prevenzione efficace che tenga conto di tutti gli aspetti di sicurezza
- **CLOUD SECURITY ALLIANCE ITALY CHAPTER –** la convenzione tra AIIC e CLOUD SECURITY ALLIANCE ITALY CHAPTER è stata firmata il 26 aprile 2012, con l'intento di collaborare per dare reciprocamente visibilità alle iniziative sviluppate autonomamente da ciascuna delle due associazioni in occasione di incontri, corsi e seminari di studio.
- **ISACA Rome Chapter** La convenzione con ISACAROMA (capitolo di Roma della *Information Systems Audit And Control Association*, associazione internazionale con circa 140.000 soci nel mondo)

è stata firmata il 7 dicembre 2018 con l'intento promuovere la collaborazione tra le due associazioni per l'organizzazione di eventi, seminari sulla cyber security e le infrastrutture critiche.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.
Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.
Potete scriverci al nostro solito indirizzo email: *segreteria@infrastrutturecritiche.it*

NUOVO GRUPPO DI LAVORO AIIC
"Resilienza delle Infrastrutture Critiche e Cambiamenti Climatici"

Il Consiglio Direttivo AIIC nella sua riunione del 19 Settembre 2022 ha approvato la nascita del GdL ***"Resilienza delle Infrastrutture Critiche e Cambiamenti Climatici"***.

Le nuove infrastrutture dovranno essere pianificate, progettate, costruite e gestite tenendo nella dovuta considerazione le minacce sistemiche che possono verificarsi nel corso della loro vita, inclusi i cambiamenti climatici, e nel rispetto dei vincoli di sviluppo sostenibile. Dovranno essere progettate e pensate per contribuire al raggiungimento degli Obiettivi di Sviluppo Sostenibile dell'Agenda 2030, in

particolare l'SDG 9 "Costruire un'infrastruttura resiliente e promuovere l'innovazione ed una industrializzazione equa, responsabile e sostenibile".

Coordinatore: Sandro Bologna
Data inizio lavori: 01.11.2022
Durata max: 12 mesi
La lista degli argomenti proposti è contenuta nel sito sociale alla pagina
https://infrastrutturecritiche.it/resilienza-delle-infrastrutture-critiche-e-cambiamenti-climatici/

Tutti i Soci AIIC che intendono partecipare sono invitati a manifestare la loro disponibilità entro il 31 Ottobre 2022, inviando una mail al Coordinatore s.bologna@infrastrutturecritiche.it e per conoscenza alla Segreteria segreteria@infrastrutturecritiche.it.

Ricordiamo che la partecipazione ai Gruppi di Lavoro AIIC è riservata ai soci AIIC in regola con il pagamento delle quote sociali.
A questo proposito, il Consiglio Direttivo ha deciso una facilitazione per chi volesse partecipare associandosi – come nuovo socio – ad AIIC, e cioè di considerare valida la quota associativa versata in questo periodo di fine 2022 anche per l'intero anno 2023.

I particolari per l'iscrizione ad AIIC sono contenuti nel sito www.infrastrutturecritiche.it.

NEWS E AVVENIMENTI

Nuova direttiva europea sulle infrastrutture critiche: punti salienti e innovazioni - Parlamento e Consiglio europeo hanno raggiunto l'accordo circa l'approvazione di nuove norme che mirano a rafforzare il livello di preparazione delle infrastrutture critiche di fronte a una serie di nuove minacce. Ecco i punti salienti e le innovazioni introdotte dalla direttiva CER.
Il 28 giugno il Parlamento Europeo e il Consiglio dell'Unione Europea hanno raggiunto un accordo circa l'approvazione della Direttiva sulla resilienza delle infrastrutture critiche (CER), proposta dalla Commissione nel dicembre 2020.
Le nuove norme hanno lo scopo di rafforzare il livello di preparazione delle infrastrutture critiche di fronte a una serie di minacce, tra cui i rischi naturali, gli attacchi terroristici, le minacce interne o il sabotaggio, nonché le emergenze sanitarie come la recente pandemia di Covid-19.
Indice degli argomenti

(continua)
https://www.cybersecurity360.it/cybersecurity-nazionale/nuova-direttiva-europea-sulle-infrastrutture-critiche-punti-salienti-e-innovazioni/
***Cybersecurity360** - Davide Agnello, Gaetano Grech, Martina Rossi - 01 Set 2022*

Popular IoT Cameras Need Patching to Fend Off Catastrophic Attacks - Several models of EZVIZ cameras are open to total remote control by cyberattackers, and image exfiltration and decryption.
At least five models of EZVIZ Internet of Things (IoT) cameras are vulnerable to a handful of vulnerabilities that could lead to threat actors accessing, decrypting, and downloading the video from the devices.
EZVIZ is a smart home security brand of cloud-connected hardware used across the globe, offering dozens of IoT security camera models. (*continua*….)
https://www.darkreading.com/attacks-breaches/popular-iot-cameras-patching-catastrophic-attacks
***DARK READING -**Dark Reading Staff- September 15, 2022*

Operazioni cibernetiche offensive: così l'Italia si prepara alla cyberwar - Il DL Aiuti ha introdotto la possibilità per i nostri servizi segreti di effettuare operazioni cibernetiche offensive per rispondere ai sempre più numerosi attacchi informatici. Ecco un'analisi della norma per comprendere le modifiche più significative al nostro ordinamento
Il costante aumento degli attacchi informatici perpetrati da soggetti di matrice statale e non e la loro sempre maggiore sofisticatezza ha portato numerosi attori internazionali ad adottare nuovi strumenti, anche legislativi, per fronteggiarli.
A livello nazionale, in un contesto di incrementata attenzione al tema della cyber security, il decreto-legge del 9 agosto 2022, n. 115 (cosiddetto "Decreto Aiuti", convertito in legge lo scorso 15 settembre 2022) ha introdotto significative modifiche al nostro ordinamento ammettendo lo svolgimento di operazioni cibernetiche offensive.
Indice degli argomenti

Nuove misure di intelligence in ambito cyber
Nello specifico, l'attuale testo dell'articolo 37, rubricato "Disposizioni in materia di intelligence", prevede la possibilità per il Presidente del Consiglio dei ministri di emanare disposizioni volte all'adozione di misure di intelligence di contrasto in ambito cibernetico.
Il ricorso a tale strumento è soggetto ad alcune condizioni: innanzitutto, ci si deve trovare in una situazione di crisi o di emergenza derivanti da minacce che coinvolgano aspetti di sicurezza nazionale.
Inoltre, le operazioni cibernetiche offensive potranno essere disposte solo nel caso in cui la situazione avversa non possa essere fronteggiata con azioni di resilienza. *(continua…)*
https://www.cybersecurity360.it/cybersecurity-nazionale/operazioni-cibernetiche-offensive-cosi-litalia-si-prepara-alla-cyberwar/
***Cybersecurity360** - Lucrezia Falciai -15 Set 2022*

Cybersicurezza, il Governo puntella il sistema di difesa: ecco tutte le novità - Dagli obblighi di notifica per gli incidenti su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro di sicurezza nazionale cibernetica all'adozione di misure di intelligence di contrasto in ambito cibernetico. Le novità del decreto Aiuti bis

Le istanze di sicurezza legate al momento geopolitico e al conflitto russo-ucraino hanno spinto il Governo a dare una sterzata al concetto di **sicurezza nazionale cibernetica.**

Gli obblighi di notifica attualmente previsti per gli incidenti aventi impatto su beni destinati a essere impiegati nel **Perimetro di sicurezza nazionale cibernetica** (beni ICT), saranno infatti estesi anche agli **incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro,** ma che sono di pertinenza di soggetti inclusi nel Perimetro.

Prevista poi la possibilità per **il Presidente del Consiglio** di autorizzare l'attuazione di **misure di intelligence** di contrasto in ambito cibernetico.

Vediamo cosa cambia nella sostanza.

Indice degli argomenti

- Il Perimetro di sicurezza nazionale cibernetica
- Notifiche degli attacchi: le novità del Decreto aiuti bis
- Le novità in tema di adozione di **misure di intelligence** di contrasto in ambito cibernetico

Il Perimetro di sicurezza nazionale cibernetica nasce con il concetto che sia possibile "identificare e designare i servizi inerenti alla sicurezza cyber nazionale" in modo univoco, chiaro e indipendente, per ciascun servizio, dal mondo che lo circonda. *(continua…)*

https://www.agendadigitale.eu/sicurezza/cybersicurezza-il-governo-puntella-il-sistema-di-difesa-ecco-tutte-le-novita/

AgendaDIGITALE *- Luisa Franchina - 19 Set 2022*

Certificazioni cyber security, la Ue cambia ancora: i nodi delle notifiche di conformità - Troppe svolte improvvise nel cyber resilience act: l'ultima in ordine di tempo è quella verso la dichiarazione di conformità, che solleva numerose domande in vista di una messa a terra che si preannuncia accidentata. Ecco i dubbi di un percorso che dovrebbe coinvolgere attivamente non solo le aziende ma anche i consumatori

Il ***cyber resilience act*** proposto dalla Commissione e in discussione al Parlamento Europeo ricorda una scena di inseguimento tra automobili in un film d'azione. L'inseguito svolta improvvisamente a tutta velocità compiendo una manovra ad angolo retto in controsterzo e si infila in un percorso che neanche vediamo, attualmente, noi seduti nella vettura degli inseguitori.

Stavamo giusto parlando di ***certificazioni di cyber security per i prodotti***, ne parliamo da anni e seguiamo con grande attenzione l'evolversi degli standard europei, numerosi, complessi e solo parzialmente arrivati alla nascita. Seguiamo anche con grande attenzione gli standard italiani, legati al CVCN che tutti sappiamo sta lavorando per rendere pubbliche le regole con le quali si potrà procedere ad acquisti di tecnologia ICT per servizi interni al Perimetro di sicurezza nazionale cibernetica e per servizi inerenti a cloud e 5G.

Anzi, dobbiamo dire che molte grandi e piccole aziende sono "alla mossa", come nel palio di Siena, in attesa delle linee guida di certificazione che consentiranno di effettuare acquisti duraturi e "impiegabili" in ambito ICT per i prossimi anni. Questo è un tema prettamente italiano, certamente, stante il momento normativo di attesa degli standard del CVCN.

Tuttavia, adesso tutti i partecipanti a questo grande "momentum" in stile paliesco si sono voltati a gomito, attratti dalla svolta in corsa della Commissione Europea verso la dichiarazione di conformità che troviamo nel cyber resilience act.

Indice degli argomenti

- La dichiarazione di conformità del cyber resilience act
- Le sanzioni
- La messa a terra delle nuove norme

La dichiarazione di conformità del cyber resilience act

Dunque? Proviamo a riassumere. Tutti prodotti che andranno sul mercato in suolo europeo e che contengono ICT in senso generale, cioè elementi digitali, dovranno rispettare **requisiti obbligatori di sicurezza informatica**, durante tutto il loro ciclo di vita. Sono inclusi tutti i dispositivi con una connessione diretta o indiretta a un altro dispositivo o alla rete, fissa o mobile, come Pc, smartphone, prodotti per la smart home, cuffie wireless, software. *(continua…)*

https://www.agendadigitale.eu/sicurezza/certificazioni-cyber-security-la-ue-cambia-ancora-i-nodi-delle-notifiche-di-conformita/

AgendaDIGITALE *- Luisa Franchina - 20 Set 2022*

Hacker Plunders $160M From Crypto Market Maker Wintermute - A hacker stole $160 million in digital assets from cryptocurrency trading firm Wintermute, its chief executive said Tuesday in an appeal for hackers to restore the funds that also contained a message that the company remains solvent. Any lender inclined to recall a loan will be paid in full, tweeted CEO Evgeny Gaevoy.

The hack affected the London-based market maker's decentralized finance operation but not its centralized finance or over-the-counter operations, Gaevoy said. The company has more than twice the stolen amount on hand in equity, he added.

Wintermute supplies liquidity to cryptocurrency trading by holding digital assets in internet-connect wallets and tapping into them when necessary to ensure the execution of large deals. The company is among the largest market makers and is backed by Lightspeed Venture Partners and Pantera Capital.

"We are (still) open to treat this as a white hat, so if you are the attacker - get in touch," Gaevoy tweeted.

Hacked cryptocurrency trading platforms often ask for stolen funds to be returned and sometimes even receive money back. *(continua…)*

https://www.bankinfosecurity.com/hacker-plunders-160m-from-crypto-market-maker-wintermute-a-20114

BANKINFOSECURITY *- Mihir Bagwe - September 20, 2022*

Would you sell your data for profit? Nearly 50% of Americans said they would - You might take your online privacy very seriously. You always connect to one of the best VPN services when surfing the net. Likewise, you also carefully read terms and conditions before clicking the 'Agree' button. You may even customize the settings of your smartphone and apps to make sure they record as less information about you as possible.

However, despite all your efforts, big tech companies are still collecting a huge amount of data about you every day. They unsurprisingly make tons of money out of it, too.

Being that data collection looks like an inevitable practice, why not gain from it yourself, then. Would you feel comfortable selling your sensitive data for a profit if you would have the means to do so?

This is exactly one of the questions that analysis firm Exploding Topics addressed to more than 1,600 Americans. And - surprise, surprise - nearly half of the respondents said they would.

Earning money from your data as a fair practice

As part of a bigger investigation, analysts from Exploding Topics reached out (opens in new tab) to 1,617 internet users living in the US to gather their views on data privacy, ownership of online content and the role of big tech companies.

Perhaps the most interesting finding is actually about the selling of personal data.

While acknowledging that these firms make a huge profit sharing users' personal data to third parties for commercial purposes, a staggering 47.9% of the respondents said they would consider selling their data for a financial gain.

The remaining half is then split between a 26.5% saying they wouldn't, and a 25.6% said to be unsure of what they would do if they have a chance to cash off their own sensitive information.

Analysts got an even stronger response when asking if users should automatically get part of the profit in case a company sells their data. Here, more than 70% agreed that it would be a fair exchange.

Which data do Big Tech collect about you?

While it's unlikely that such a practice will gain a foothold in the big tech sector anytime soon, you can at least make some more conscious choices on which information to share and with whom. For this, it's important to exactly know the types of personal data these companies hold about their users. *(continua…)*

https://www.techradar.com/news/would-you-sell-your-data-for-profit-nearly-50-of-americans-said-they-would?utm_campaign=FE54DD43-74DE-4BF6-9900-7F0A89D648D2

***TECHRADAR**-Chiara Castro- 21 sept 2022*

Cybersecurity, Zoom ha una serie di vulnerabilità di media gravità - Zoom ha una serie di vulnerabilità di media gravità. Il CERT-In: Sono legate alll' Improper Access Control e permettono a un attaccante remoto di accedere alle riunioni in stealth

Zoom ha una serie di vulnerabilità di media gravità (CVE-2022-28760, CVE-2022-28759 e CVE-2022-28758, Improper Access Control), che possono essere sfruttate da un attaccante in remoto per accedere alle riunioni in corso senza essere visibile ai partecipanti e di sottrarre contenuti.

Lo denunciano gli esperti di cybersecurity del CERT-In (India). La piattaforma è al corrente delle falle e ha emesso nei giorni scorsi un avviso, in cui si comunica che queste coinvolgono tutte le versioni della piattaforma precedenti alla 4.8.20220815.130. Di conseguenza, si raccomanda al più presto di aggiornare Zoom alla versione più recente.

https://www.difesaesicurezza.com/cyber/cybersecurity-zoom-ha-una-serie-di-vulnerabilita-di-media-gravita/?ct=t(RSS_EMAIL_CAMPAIGN)

***Difesa e Sicurezza -** Francesco Bussoletti - 23 Settembre 2022*

How Europe Is Using Regulations to Harden Medical Devices Against Attack - Manufacturers need to document a medical device's intended use and operational environment, as well as plan for misuse, such as a cyberattack.

Due to the increasing concerns about medical devices' cybersecurity risks, European Union regulators put forward a new set of market entry requirements for medical devices and in vitro diagnostic medical devices to reduce the risk of patient harm as a result of a cyber incident, as well as protect national health systems.

EU regulators are raising the bar on cybersecurity requirements with the European Union Medical Device Regulation (MDR) and the European Union In Vitro Diagnostic Regulation (IVDR), which went into effect May 26, 2021. The regulations are intended to "establish a robust, transparent, predictable

and sustainable regulatory framework ... which ensures a high level of safety and health whilst supporting innovation."

Organizations have until May 26, 2024, or when their current market certification expires, to make the necessary changes to their quality management systems and technical documentation to comply with the new requirements. Despite the number of assessment processes and standards and guidance documents that have been provided, medical device manufacturers, providers, and certification services may not be ready in time.

More than 90% of currently valid AIMDD/MDD certificates will expire by 2024, so a significant number of existing devices need to be reapproved, in addition to new devices entering the market. It is estimated that 85% of products currently on the market today still require new certification under MDR.IVDR. Considering that the process takes 13 to 18 months, companies need to start the process now in order to meet the 2024 deadline.

Setting Instructions for Use

In general, cybersecurity processes are not that different from general device performance and safety processes. The goal is to assure (through verification and validation) and demonstrate (through documentation) device performance, risk reduction and control, and minimization of foreseeable risks and undesirable side effects through risk management. Combination products or interconnected devices/systems also require management of the risks that result from interaction between software and the IT environment.

The Medical Device Coordination Group's MDCG-16 Guidance on Cybersecurity for medical devices explains how to interpret and fulfill cybersecurity requirements under MDR and IVDR. Manufacturers are expected to take into account the principles of the secure development life cycle, security risk management, and verification and validation. Further, they should provide minimum IT requirements and expectations for cybersecurity processes, such as installation and maintenance in their device's instructions for use. "Instructions for use" is a highly structured required section of the certification application manufacturers must file. *(continua….)*

https://www.darkreading.com/edge-articles/how-europe-is-using-regulations-to-harden-medical-devices-against-attack

DARKREADING - *Axel Wirth - September 23, 2022*

Espionage Group Wields Steganographic Backdoor Against Govs, Stock Exchange - APT group Witchetty (aka LookingFrog) has exploited the ProxyShell and ProxyLogon vulnerabilities to gain initial access and deploy new custom cyber tools against government agencies and a stock exchange.

An emerging cyber-espionage threat group has been hitting targets in the Middle East and Africa with a novel backdoor dubbed "Stegmap," which uses the rarely seen steganography technique to hide malicious code in a hosted image.

Recent attacks show the group — called Witchetty, aka LookingFrog — fortifying its tool set, adding sophisticated evasion tactics, and exploiting known Microsoft Exchange vulnerabilities ProxyShell and ProxyLogon. Researchers from Symantec Threat Hunter observed the group installing webshells on public-facing servers, stealing credentials, and then spreading laterally across networks to propagate malware, they revealed in a blog post published Sept. 29.

In attacks between February and September, Witchetty targeted the governments of two Middle Eastern countries and the stock exchange of an African nation in attacks that used the aforementioned vector, they said.

ProxyShell is comprised of three known and patched flaws — CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207 — while ProxyLogon is comprised of two, CVE-2021-26855 and CVE-2021-

27065. Both have been exploited widely by threat actors since they were first revealed in August 2021 and December 2020, respectively — attacks that persist as many Exchange Servers remain unpatched. Witchetty's recent activity also shows that the group has added a new backdoor to its arsenal, called Stegmap, which employs steganography — a stealthy technique that stashes the payload in an image to avoid detection.

How the Stegmap Backdoor Works

In its recent attacks, Witchetty continued to use its existing tools, but also added Stegmap to flesh out its arsenal, the researchers said. The backdoor uses steganography to extract its payload from a bitmap image, leveraging the technique "to disguise malicious code in seemingly innocuous-looking image files," they said.

The tool uses a DLL loader to download a bitmap file that appears to be an old Microsoft Windows logo from a GitHub repository. "However, the payload is hidden within the file and is decrypted with an XOR key," the researchers said in their post.

By disguising the payload in this way, attackers can host it on a free, trusted service that is far less likely to raise a red flag than an attacker-controlled command-and-control (C2) server, they noted.

The backdoor, once downloaded, goes on to do typical backdoor things, such as removing directories; copying, moving, and deleting files; starting new processes or killing existing ones; reading, creating, or deleting registry keys, or setting key values; and stealing local files.

In addition to Stegmap**,** Witchetty also added three other custom tools — a proxy utility for connecting to command-and-control (C2), a port scanner, and a persistence utility — to its quiver, the researchers said. *(continua…)*

https://www.darkreading.com/attacks-breaches/espionage-steganographic-backdoor-against-govs-stock-exchange

DARKREADING -*Elizabeth Montalbano - September 29, 2022*

Resilienza operativa nelle organizzazioni: come evolve la normativa (e non solo) - Il regolamento DORA costituisce solo uno dei tasselli di una articolata serie di normative, in particolare nel mondo finanziario, che suggeriscono come rendere un'organizzazione sempre più resiliente. Suggerimenti che, se adeguatamente adattati, sono in realtà utili in qualunque settore.

Come più volte ho ricordato sia su questa testata, sia in altri articoli, il mondo della continuità operativa e della cyber security trova ampio spazio di trattazione e regolamentazione nell'ambito finanziario. Il Regolamento DORA rappresenta, in questo senso, l'ultimo dei tasselli normativi.

Le motivazioni sono immediatamente comprensibili a tutti; si tratta di un settore nel quale le probabilità di essere oggetto di un attacco da parte di qualche malintenzionato sono rilevanti, in conseguenza di quello che è il particolare "prodotto" trattato.

In considerazione, inoltre, del ruolo assolutamente strategico che tale settore riveste, il legislatore (o meglio, i vari legislatori coinvolti) sono molto attivi nel produrre normative che vincolano gli istituti finanziari.

Tali normative hanno la finalità di garantire un alto livello di sicurezza e una elevata capacità di resilienza rispetto a qualunque tipologia di attacco o, più in generale, di evento che possa minacciare la stabilità e la capacità di operare delle banche.

Indice degli argomenti

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

https://www.cybersecurity360.it/soluzioni-aziendali/resilienza-operativa-nelle-organizzazioni-come-evolve-la-normativa-e-non-solo/
Cybersecurity360 *- Giancarlo Butti – 5 ottobre 2022*

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link *http://www.infrastrutturecritiche.it/new/per-iscriversi/*

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare I nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Palestro 95 – 00185 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	Si informa che AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirti al gruppo è sufficiente usare il seguente link: http://www.linkedin.com/ groups/96335
Versione stampabile della newsletter	Nella sezione "Newsletter"del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Comitato di Redazione
Alberto Traballesi
Glauco Bertocchi
Silvano Bari
ai quali potete inviare suggerimenti e quesiti scrivendo a:
segreteria@infrastrutturecritiche.it