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 2020	N. 09/ 2020	Ottobre 2020

L' IoT nel contesto delle Infrastrutture Critiche

E' da qualche anno che la dicitura IoT (Internet of Things in inglese e Internet delle Cose in italiano) è usata con significati diversi in domini diversi. Per applicazioni domestiche per indicare l'automazione delle funzioni di gestione della casa, per applicazioni industriali per indicare l'automazione delle funzioni di gestione degli impianti industriali, e così via nelle applicazioni sanitarie, sicurezza delle città, gestione del traffico, ecc. Non da ultima nella gestione dei Servizi Essenziali forniti dalle Infrastrutture Critiche Nazionali.
Ma quale è la percezione comune di un IoT? Troppo spesso si confonde il concetto di IoT con quello di componente. Da sola la fotocamera posizionata sul cancello della villetta al mare non è un IoT, ma la stessa fotocamera collegata via Internet al sistema di allarme della casa e/o allo *smartphone* del proprietario della villetta, costituisce un IoT. Da qui la conclusione che IoT è un Sistema aperto il cui perimetro non è riconducibile a dei confini rigidamente determinati, e quindi difendibili nel senso classico. Molteplici sono i punti di attacco che possono essere usati da male-intenzionati, comunemente indicati come *hackers*.
Quindi quali sono i problemi delle soluzioni IoT per applicazioni critiche? E' nella definizione di strategie di sicurezza, intesa nelle due accezioni di *security* e di *safety*, e di trattamento dei dati personali, indicata comunemente come *privacy*.
Sono proprio questi tre aspetti che sono affrontati dal Rapporto AIIC dedicato agli IoT nel contesto delle Infrastrutture Critiche (IC), ultimo di una serie di Rapporti AIIC dedicati ai vari aspetti delle IC, iniziata nel 2015 con un Rapporto dedicato alla valutazione della Resilienza delle IC, quando il concetto di Resilienza oggi tanto abusato, non era ancora di comune uso.
Dopo una breve introduzione, rivolta a fissare il concetto di IoT come Sistema e non come componente, in cui si possono distinguere almeno tre livelli: componenti in campo che contribuiscono alla generazione dei dati, componenti per le funzioni di aggregazione dei dati e componenti per la gestione e la presentazione delle informazioni derivate dai dati acquisiti in campo, il tutto connesso via reti di trasmissione dati che utilizzano il protocollo TCP/IP, standard de facto della rete Internet.
Il corpo centrale del rapporto è dedicato all'analisi dei problemi legati a come garantire gli aspetti di *security, safety e privacy* dei Sistemi IoT per la gestione dei Servizi Essenziali forniti dalle Infrastrutture Critiche Nazionali. Analisi sostenuta da precisi riferimenti allo stato dell'arte, come rappresentato dalle maggiori realtà di definizione di *Best Practices* e Standard internazionali quali ENISA, NIST, ISO, IEEE. Il lavoro è sostenuto da un capitolo dedicato alla definizione di possibili scenari di attacchi cyber per diversi domini di interesse, dall'industria all'energia, dai trasporti alla gestione del traffico, per concludersi con un capitolo dedicato all'analisi dei problemi legati all'introduzione dei Sistemi IoT nel dominio della salute, generalmente riferito con il termine inglese *Healthcare.*

Sandro Bologna
Laureato in fisica alla Sapienza, Università di Roma, è membro del Consiglio Direttivo dell'AIIC. Tra le principali attività di ricerca attuali si citano la valutazione della sicurezza, protezione e resilienza di infrastrutture critiche, con particolare riferimento agli aspetti di analisi delle vulnerabilità alle minacce di origine naturale e umana e alla modellistica dei diversi fattori che concorrono a costituire una infrastruttura.

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

ATTIVITA' DELL'ASSOCIAZIONE

Rinnovo associativo per l'anno 2021

Si ricorda a tutti i soci che il 31 dicembre 2021 scadrà il periodo associativo. Invitiamo tutti i soci a rinnovare per tempo l'associazione versando il relativo contributo, ormai inalterato da anni.
La quota per il rinnovo individuale è di euro 40 e può essere versata con bonifico sul c/c presso Banca Intesa Business, Coordinate bancarie IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando "rinnovo socio ordinario nome e cognome anno 2021".

Per i nuovi iscritti l'importo da pagare è di € 60,00 e, come stabilito dall'ultimo Consiglio Direttivo, le iscrizioni pervenute dal 1 novembre 2020 in poi avranno una durata valida per tutto il 2021 (perciò scadenza 31.12.2021). Le quote e le modalità di rinnovo per i soci collettivi – così come le indicazioni per chi vuole iscriversi come nuovo socio - sono contenute nel sito AIIC al link
http://www.infrastrutturecritiche.it/new/per-iscriversi/

Ricordiamo che la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2021. Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione, versando in più il relativo contributo per le spese di segreteria.

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da inserire, per esempio, in newsletter o nel sito AIIC.
In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIIC: in tal caso – però – la partecipazione di AIIC ad un evento deve essere decisa dal Consiglio Direttivo, pertanto siete pregati di contattare il CD con ragionevole anticipo, alla mail segreteria@infrastrutturecritiche.it
In caso non fosse possibile la partecipazione a nome AIIC, vi invitiamo ad indicare, nel profilo professionale, la vostra appartenenza ad AIIC.

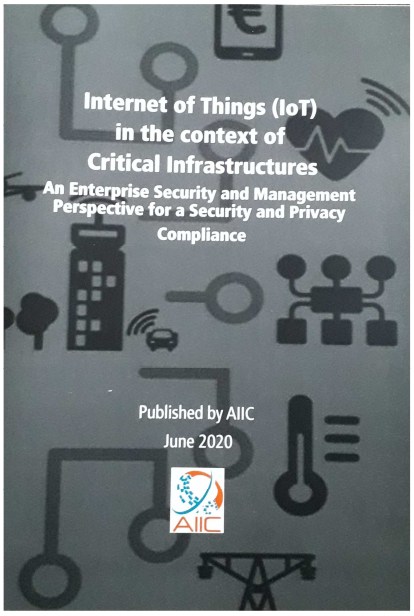
AIIC ha sottoscritto convenzioni di collaborazione con altre Associazioni. In particolare con:

- **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 ed autonomi 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.

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

ATTIVITA' DELL'ASSOCIAZIONE

GDL AIIC
su Internet of Things



Il Gruppo di Lavoro AIIC "**Internet of Things (IoT) in the context of Critical Infrastructures: An Enterprise Security and Management Perspective for a Security and Privacy Compliance"** ha concluso la sua attività.
Il Gdl è stato coordinato da Sandro Bologna e ha visto la partecipazione dei soci Silvano Bari, Glauco Bertocchi, Luigi Carrozzi, Luisa Franchina, Francesco Ressa, Angelo Socal, Alberto Traballesi.
Il rapporto è stato stampato come pubblicazione cartacea ed è possibile anche il download in formato pdf dal sito AIIC al link
https://www.infrastrutturecritiche.it/wp-content/uploads/2020/09/GdL-Internet-of-Things_rev-2020.08.12-2.pdf

I soci che volessero ottenere una copia cartacea del rapporto dovranno contattare la segreteria AIIC per concordare le modalità di ritiro o di spedizione.

Come riportato in altra notizia, il contenuto della pubblicazione sarà illustrato nel prossimo Colloquia che si terrà il giorno 26 ottobre in modalità webinar.

COLLOQUIA
INTERNET OF THINGS NEL CONTESTO DELLE INFRASTRUTTURE CRITICHE
LUNEDI' 26 OTTOBRE 2020
Ore 15.00 – 16.30

Siamo felici di comunicare che, dopo una lunga pausa dovuta ai noti eventi sanitari, riprenderemo i nostri incontri periodici sui vari temi legati alla protezione delle infrastrutture critiche.
I prossimi Colloquia, organizzati come di consueto con la collaborazione della Università Roma Tre, si svolgeranno in modalità webinar, con la speranza – comunque – di poterci incontrare di nuovo in presenza in un prossimo futuro che ci auguriamo non essere troppo lontano.

Il nuovo Colloquia verterà sul tema dell'**Internet of Things nel contesto delle Infrastrutture Critiche** e vedrà, tra l'altro, l'illustrazione dell'ultimo rapporto AIIC su tale argomento, ad opera del coordinatore del gdl Sandro Bologna e degli altri partecipanti. Seguirà il punto di vista, sempre su tale argomento, di un noto provider di soluzioni ICT.

L'appuntamento è quindi per il **giorno lunedì 26 ottobre alle ore 15.00** via web. L'evento è aperto a tutti gli interessati ma per motivi di collegamento è necessario inviare una mail di adesione alla segreteria AIIC: si riceverà la conferma di partecipazione e le indicazioni per il collegamento.

CALL FOR IDEAS

AIIC vuole lanciare anche quest'anno un Gruppo di Lavoro e sollecita i soci e i simpatizzanti a fornire idee su possibili argomenti da cui sviluppare un report come avvenuto negli anni passati. Tutti i suggerimenti saranno attentamente valutati dal Consiglio Direttivo purché i promotori siano disponibili a contribuire attivamente alla riuscita del GDL.

NEWS E AVVENIMENTI

Città e comunità sostenibili: il supporto della normativa tecnica per definire un sistema di gestione efficace. Un sistema di gestione per rendere le città più resilienti, smart e sostenibili: i contenuti della UNI ISO 37101:2019 - Per rispondere in modo ottimale al fenomeno dell'urbanizzazione è fondamentale che le autorità adottino un sistema di gestione efficace delle comunità, con l'obiettivo di avere città inclusive, sane, resilienti e sostenibili.
Nel 2016 l'Organizzazione internazionale per la normazione (ISO) ha definito i requisiti per un sistema di gestione per lo sviluppo sostenibile nelle comunità pubblicando la norma ISO 37101. Successivamente, nel 2019, è stata pubblicata la norma ISO 37104 che introduce metodologie e indicazioni per l'implementazione pratica della ISO 37101.
Abbiamo formulato alcune domande al Dr. Giacomo Riccio - Funzionario Tecnico Direzione Normazione UNI - per comprendere e approfondire meglio i contenuti delle due norme.
https://www.ingenio-web.it/28144-citta-e-comunita-sostenibili-il-supporto-della-normativa-tecnica-per-definire-un-sistema-di-gestione-efficace?utm_term=39315+-+http%3A%2F%2Fingenio-web.it%2F28144-citta-e-comunita-sostenibili-il-supporto-della-normativa-tecnica-per-definire-un-sistema-di-gestione-efficace&utm_campaign=La+Gazzetta+di+INGENIO&utm_medium=email&utm_source=MagNews&utm_content=3770+-+2080+%282020-09-11%29
***INGENIO** - Cuoghi Dalila - Riccio Giacomo 08/09/2020*

La definizione di RISCHIO e la sua valutazione - Qualche giorno fa è stato messo online sui siti istituzionali del Dipartimento della Protezione civile e del Ministero dell'Istruzione (MI) il volume "La Protezione civile in Italia". Nel testo dopo una panoramica sulle competenze e sulle attività del servizio del Dipartimento della Protezione civile, si passa a una rappresentazione della fragilità del territorio italiano rispetto ai diversi rischi. Ma cosa è innanzitutto il RISCHIO? Di seguito una definizione del Rischio tratta dal volume sopracitato.
https://www.ingenio-web.it/28121-la-definizione-di-rischio-e-la-sua-valutazione?utm_term=39205+-+https%3A%2F%2Fwww.ingenio-web.it%2F28121-la-definizione-di-rischio-e-la-sua-

valutazione&utm_campaign=La+Gazzetta+di+INGENIO&utm_medium=email&utm_source=MagNews&utm_content=3761+-+2077+%282020-09-08%29
Redazione INGENIO - *07/09/2020*

CISA: Chinese state hackers are exploiting F5, Citrix, Pulse Secure, and Exchange bugs
CISA says attacks have started a year ago and some have been successful.
The Cybersecurity and Infrastructure Security Agency (CISA) has published a security advisory today warning of a wave of attacks carried out by hacking groups affiliated with China's Ministry of State Security (MSS).
CISA says that over the past year, Chinese hackers have scanned US government networks for the presence of popular networking devices and then used exploits for recently disclosed vulnerabilities to gain a foothold on sensitive networks.
The list of targeted devices includes F5 Big-IP load balancers, Citrix and Pulse Secure VPN appliances, and Microsoft Exchange email servers.
For each of these devices, major vulnerabilities have been publicly disclosed over the past 12 months, such as CVE-2020-5902, CVE-2019-19781, CVE-2019-11510, and CVE-2020-0688, respectively.
According to a table summarizing Chinese activity targeting these devices published by CISA today, some attacks have been successful and enabled Chinese hackers to gain a foothold on federal networks.
https://www.zdnet.com/article/cisa-chinese-state-hackers-are-exploiting-f5-citrix-pulse-secure-and-exchange-bugs/
Zero Day- *Catalin Cimpanu-September 14, 2020*

Breach of COVID-19 Test Data Undermines Pandemic Response 'Human Error' Results in 18,000 Individuals' Test Results Being Exposed in Wales What's one of the worst things that can happen during a pandemic? The answer is anything that gives people less trust in their public health system to handle the crisis, potentially leading to lower compliance with essential government guidance and undercutting efforts to eradicate the outbreak. Enter a U.K. data breach that has exposed personally identifiable information for every one of the 18,105 residents of Wales who tested positive for COVID-19 from Feb. 27 to Aug. 30. "Don't let this mistake put you off getting tested." Public Health Wales, the national public health agency, first disclosed the breach on Monday, saying it was the result of "individual human error" and had occurred on Aug. 30 after the PII was "uploaded by mistake to a public server where it was searchable by anyone using the site." Public Health Wales says it immediately excised the data after being alerted to the breach. "In the 20 hours it was online it had been viewed 56 times," the agency says.
The health agency says the exposed information falls into two categories:

- **Lower risk of identification:** For 16,179 individuals, exposed information "consisted of their initials, date of birth, geographical area and gender, meaning that the risk they could be identified is low."
- **Higher risk of identification:** The remaining 1,926 individuals live in nursing homes or supported housing - including homelessness hostels, refuges, long-term accommodation for individuals unable to live in the community - and the exposed information included the above, as well as the name of the setting in which they live.

For the individuals for whom more information was exposed, "the risk of identification for these individuals therefore is higher but is still considered low," Public Health Wales says, noting that the U.K.'s Information Commissioner's Office has been alerted, and a full investigation is underway.....

https://www.bankinfosecurity.com/blogs/breach-covid-19-test-data-undermines-pandemic-response-p-2938
Bankinfosecurity *-Mathew J. Schwartz -• September 15, 2020*

IL CASO IN GERMANIA Che ci insegna il primo decesso per attacco hacker
Doveva succedere, era solo questione di tempo. Ed è successo. Una donna, con un estremo bisogno di cure mediche, viene trasportata in ambulanza verso l'ospedale Universitario di Duesseldorf, in Germania, ma a seguito di un attacco ransomware l'ospedale non è in grado di gestire la paziente, e l'ambulanza fa rotta verso l'ospedale di Wuppertal, a circa 30 km dalla destinazione iniziale. La paziente muore durante il trasferimento.
Indice degli argomenti
- La vulnerabilità ignorata dagli ospedali
- I consigli

La vulnerabilità ignorata dagli ospedali
Il problema, ovviamente, risiede nel fatto che l'ospedale di Duesseldorf fosse sotto attacco ransomware, con più di 39 server implicati. Il vero punto però è dato dal fatto che la vulnerabilità posta sotto attacco (al gateway Citrix della rete) era stata segnalata da BSI (l'authority per la Cyber Security tedesca) come un punto attaccabile dal ransomware direttamente alle organizzazioni tedesche il giorno prima. Per giunta, era vulnerabilità nota già da gennaio come possibile tramite di pericolosi attacchi ransom.
L'incidente segna la prima morte umana segnalata che sia indirettamente causata da un attacco ransomware (anche se come scritto risultano studi che correlano un aumentato tasso di mortalità con Wannacry).
Le autorità tedesche stanno cercando una corresponsabilità tra l'attacco ransomware e il tempo di inattività dell'ospedale, che, se verificata, potrebbe portare a un caso di omicidio.
Secondo il notiziario tedesco RTL, la richiesta di riscatto è stata ritirata quando la polizia ha preso in mano la vicenda e sono state fornite all'ospedale le chiavi di decrittazioni e i tecnici (non solo dell'ospedale ma dell'intero plesso universitario che era stato colpito) stanno ripristinando i sistemi.
I consigli
La storia è nota e riguarda anche l'Italia, come da recenti attacchi a nostri ospedali. Queste strutture di solito non curano bene il reparto IT, né internamente né con contratti esterni per manutenzione e update; a causa di risorse limitate e anche probabilmente per scarsa sensibilità cyber…….
https://www.agendadigitale.eu/sicurezza/che-ci-insegna-la-prima-morte-per-attacco-hacker/
Agenda Digitale- *Walter Rocchi -18 Set 2020*

Smart Building: ecco le tecnologie che rendono più intelligenti i nostri edifici - Smart Home, IoT, edifici connessi: un tema ricorrente prima che scoppiasse l'emergenza sanitaria sia dal punto di vista del comfort sia della sostenibilità. La pandemia ha frenato il desiderio di vivere in case sempre più intelligenti o invece lo ha amplificato? Quello che sappiamo per certo è che la qualità della vita all'interno delle nostre case è diventata una priorità. Una qualità che non si traduce solo nella ricerca di immobili più grandi e possibilmente dotati di terrazzi e giardini, ma anche in una maggior attenzione verso quelle tecnologie che migliorano il nostro stile di vita, i consumi e l'impatto sull'ambiente delle case in cui viviamo. Grazie alle tecnologie digitali e alla loro integrazione in applicazioni IoT, è possibile controllare, ad esempio, illuminazione, temperatura, consumi, ingressi e uscite in ogni ambiente dell'edificio, tutto questo non solo in termini di comfort ma anche di efficientamento energetico, e proporre servizi innovativi in risposta a nuove esigenze. Quali sono quindi le tecnologie alla base di un edificio connesso, sostenibile e intelligente?

https://www.ingenio-web.it/28339-smart-building-ecco-le-tecnologie-che-rendono-piu-intelligenti-i-nostri-edifici?utm_term=39646+-+https%3A%2F%2Fwww.ingenio-web.it%2F28339-smart-building-ecco-le-tecnologie-che-rendono-piu-intelligenti-i-nostri-edifici&utm_campaign=La+Gazzetta+di+INGENIO&utm_medium=email&utm_source=MagNews&utm_content=3809+-+2098+%282020-09-28%29
INGENIO *- Samorì Chiara 24/09/2020*

Cybersecurity: Your supply chain is now your weakest link

"Criminals don't just give up, they look for easier ways in," ex-GCHQ boss Robert Hannigan tells ZDNet - and that easy way in is via your third-party suppliers. More than 80% of organisations have experienced a data breach as a result of security vulnerabilities in their supply chains, as cyber criminals take advantage of the poor security of smaller vendors as a means of gaining access to the networks of large organisations.

Research by cybersecurity company BlueVoyant found that organisations have an average of 1,013 vendors in their supplier ecosystem – and that 82% of organisations have suffered a data breach in the past 12 months due to cybersecurity weakness in the supply chain.

But, despite the risk posed by security vulnerabilities in the supply chain, a third of organisations have little to no indication if hackers had got into their supply chain, meaning that they may not find out that they've been the victim of an incident until it's too late.

Large companies are likely to be better protected than smaller companies, which means hackers are increasingly turning towards their suppliers as a means of infiltrating the network in a way that will often go unnoticed.

"Very often people think, well, what are our most critical suppliers and inevitably they end up with their top ten being some of the world's biggest names, like cloud providers. But that's not where the threat comes from," said Robert Hannigan, chairman of BlueVoyant International, told ZDNet. "It's much more likely that the real threat is going to come from a much smaller company you've never heard of but which is connected to your network," said Hannigan, who was previously director of GCHQ.

An example of this was seen in 2017 when the NotPetya attack infected organisations around the world, which was apparently first spread using the hijacked software-update mechanism of an accounting software company. The attack quickly spread out of control and took down networks of organisations across Europe and beyond. "Who would have thought with NotPetya that some accountancy software being updated would lead to massive disruption across Europe. It wasn't a top supplier for any of the companies that were hit, but it led to huge damage and interruption," said Hannigan. Other attacks against the supply chain are much more subtle, with cyber criminals infiltrating the vendor with malware or phishing emails and taking over accounts – which they then use as as a gateway to breaching the larger organisation, especially if there's already a trusted relationship between them.

This was the case when a utilities company suffered a data breached when cyber criminals targeted it via its law firm, compromising the account of someone at the firm and using that to compromise the utility company……

https://www.zdnet.com/article/cybersecurity-your-supply-chain-is-now-your-weakest-link/
Zero Day *-Danny Palmer -| September 24, 2020*

Gli 007 italiani in prima fila per la cybersecurity europea (e Parigi applaude)

Al via la seconda edizione di Blue OLEx 2020, esercitazione di sicurezza cibernetica europea. I servizi di Roma e Parigi (Dis e Anssi) in prima fila. Il capo degli 007 transalpini sulla novità dell'anno, la rete CyCLONe: "Francia e Italia le forze trainanti"

Italia e Francia assieme in prima linea per la cybersecurity europea (e i nostri 007 hanno incassato anche il plauso, nient'affatto scontato, dei colleghi francesi).

Ieri è iniziata la seconda edizione di Blue OLEx 2020, l'esercitazione di sicurezza cibernetica a livello operativo, promossa dall'Agenzia europea per la cybersecurity (Enisa), in collaborazione con la Commissione europea. I lavori, organizzati quest'anno dai Paesi Bassi, si svolgono online, con la partecipazione dei rappresentanti delle autorità cyber nazionali dei 27 Paesi membri. Per l'Italia, come nella precedente edizione, c'è il Dipartimento delle informazioni per la sicurezza (Dis) della presidenza del Consiglio dei ministri.

Gli obiettivi sono due. Primo: testare la capacità degli Stati membri in caso di eventi cibernetici in Europa. Secondo: rafforzare la cooperazione tra le autorità nazionali di cybersecurity, la Commissione europea ed Enisa.

Tra le novità di quest'anno c'è il lancio ufficiale di CyCLONe (Cyber Crisis Liaison Organisation Network), la rete di risposta rapida alle crisi e agli incidenti cyber transfrontalieri su larga scala. Si tratta di un risultato conseguito grazie al lavoro svolto in particolare dall'Italia, attraverso il Dis, e dalla Francia con l'Anssi (l'Agenzia francese per la sicurezza dei sistemi informatici), che hanno guidato i lavori nell'ambito del Nis Cooperation Group. "Forti della loro esperienza nazionale, Francia e Italia sono state le forze trainanti per la costruzione della rete CyCLONe", ha dichiarato Guillaume Poupard, direttore generale dell'Anssi.

L'intento di CyCLONe, con la Germania primo coordinatore in quanto presidente di turno del Consiglio dell'Unione europea, è l'implementazione del "meccanismo europeo di risposta rapida alle crisi e agli incidenti cyber transfrontalieri su larga scala e a supportare le strutture di cybersecurity, rafforzando la collaborazione sia a livello tecnico, per esempio tra gli Csirt, ossia i team di prevenzione e risposta agli incidenti cibernetici, sia a livello politico". L'esperienza acquisita durante i test di Blue OLEx 2020 contribuirà ad alimentare il novero delle procedure operative standard di CyCLONe, modellandone le future esercitazioni a livello operativo.

A fine febbraio, a Zagabria, le agenzie di intelligence di 23 Paesi europei avevano firmato una lettera di intenti per sancire la nascita del College dell'Intelligence in Europa (Ice), il cui segretariato avrà sede a Parigi, e la presidenza sarà a turno, su base volontaria degli Stati aderenti e della durata di un anno….

https://formiche.net/2020/09/dis-cyber-italia-francia/

FORMICHE -*Gabriele Carrer - 30/09/2020*

Ransomware, boom in Italia: come prevenire e gestire un attacco. Gli attacchi ransomware stanno caratterizzando questo periodo, nella sicurezza informatica italiana. U tipo di attacco informatico gestito da organizzazioni capaci di studiare approfonditamente il mercato per poter individuare le vittime. Ecco come agiscono e cosa fare per prevenire e dopo un incidente Il ransomware non vuole lasciare in pace l'Italia e ora è stagione soprattutto di Emotet, di cui vari ricercatori (Darktrace, Exprivia…) e lo Csirt rilevano sempre nuove campagne di malspam. Il cyber security hunter JAMESWT ha rilevato qualche giorno fa campagne mail che usavano false fatture Enel Energia come esca in allegato o presunte comunicazioni socio-sanitarie, sempre in Italia.

Un ransomware ha appena colpito Luxottica e il gruppo Carraro (multinazionale nel comparto delle macchine agricole della provincia di Padova), in questo secondo caso costringendo settecento dipendenti alla cassa integrazione per il blocco della produzione.

Indice degli argomenti

- Perché il ransomware si mostra così efficace
- Come prevenire o gestire un incidente
- Cyber security: la situazione in Italia
- Il pericoloso ritorno del trojan bancario

Perché il ransomware si mostra così efficace

Questa "popolarità" del ransomware non deve sorprendere. Il ransomware è uno strumento a bassa complessità e ad alto ritorno per i criminali.

Nel mondo informatico quello che nel mondo fisico è definito "cavallo di ritorno", ossia la richiesta di pagamento di un riscatto rivolta a chi ha subito un furto per riottenere ciò che è stato rubato. E come nel mondo fisico, dove questa "abitudine" illegale nasce, più critico è il servizio, maggiore è la possibilità che questo diventi interessante agli occhi di un criminale.

Per rendere efficace un attacco di tipo ransomware sono necessarie organizzazioni capaci di studiare approfonditamente il mercato per poter individuare le vittime. Ed è proprio qui che si trova la principale differenza tra mondo fisico e mondo digitale. Nel mondo fisico, infatti, la vittima è inequivocabilmente unica e specificamente individuata. Nel mondo digitale invece, pur non escludendo che le vittime possano essere mirate, queste possono essere svariate e spesso sono quelle meno consapevoli della minaccia a cui sono esposte.

Una volta individuata la vittima, vanno costruiti o acquistati gli strumenti necessari per sviluppare l'attacco. La tecnica più utilizzata è quella del cryptolocker, un ransomware che cripta il dato vitale (ma spesso anche altri dati) e chiede un riscatto alla vittima per la decriptazione. Ma vi sono anche altre tipologie di ransomware. Ad esempio, vi sono attacchi consistenti nel minacciare il possessore di un portale B2C/servizio internet in genere di un attacco di tipo DDoS verso il servizio che renderebbe lo stesso inutilizzabile, o attacchi consistenti nel modificare le password di accesso a servizi molto importanti. Si tratta di tecniche di attacco molto complesse: l'attaccante deve rendere inutilizzabile il servizio lasciando però il dispositivo agonizzante ed in grado di poter essere utilizzato per richiedere il riscatto e ottenere della criptovaluta, senza la quale questa attività servirebbe a poco. Quindi l'attaccante deve preoccuparsi di distribuire il malware e per far questo utilizza spesso campagne di social engineering e phishing……..

https://www.agendadigitale.eu/sicurezza/ransomware-come-prevenire-e-gestire-un-attacco/

Agenda Digitale *- Domenico Raguseo -01 Ott 2020*

Una gara per giovani hacker (ma etici) Al via, per la prima volta online, la competizione finale di CyberChallenge.IT, il programma italiano di formazione per i giovani talenti della sicurezza informatica, organizzato dal Laboratorio Nazionale Cybersecurity del Cini (Consorzio Interuniversitario Nazionale per l'Informatica). Giunta alla quarta edizione, la gara costituisce l'evento finale del corso di formazione e sviluppo di competenze specialistiche legate al mondo della cybersecurity che ha coinvolto 560 allievi, tra i 16 e i 23 anni, da gennaio a maggio. Nonostante la pandemia globale, a causa della quale l'evento sarà in remoto, gli hacker etici del laboratorio si sono confrontati in una gara durante la quale hanno dovuto sfruttare tutte le proprie competenze nei campi della crittografia, della sicurezza delle reti e delle infrastrutture hardware e software.

Nel secondo giorno di attività, oggi, gli otto team risultati migliori nella giornata precedente hanno esposto delle presentazioni divulgative legate al mondo della sicurezza informatica, di fronte a una giuria composta da istituzioni, esperti di comunicazione e da un rappresentante di ciascuna delle aziende sponsor Platinum che, insieme agli sponsor Gold e Silver, ogni anno permesso la realizzazione dell'evento (Platinum: Accenture, Aizoon, Blu5 Group, Eni, Exprivia, IBM, KPMG, Leonardo, Ntt Data,

Numera, Telsy; Gold: Bip Consulting, Cisco, Banca Monte dei Paschi di Siena, Negg, Novanext, PwC; Silver: Digi-One, Ict Cyber Consulting).
I migliori tra gli hacker etici emersi durante CyberChallenge.IT potranno essere successivamente invitati a far parte di TeamItaly, la Squadra Nazionale di Cyberdefender, che partecipa annualmente alla European Cybersecurity Challenge (Ecsc) e che nell'ultima edizione, lo scorso ottobre a Bucarest, ha conquistato il podio meritando il secondo posto……..
https://formiche.net/2020/10/hacker-ict-gara-cyber-challenge/
***FORMICHE** - Federica De Vincentis - 02/10/2020*

Cyber pirates: Shipping industry under second IT attack in a week
UN's International Maritime Organization says it suffered a 'sophisticated' cyber-attack against IT systems.
The cyber-attack on the International Maritime Organization follows another data breach at France-based CMA CGM, the world's fourth-largest container liner by capacity [File:Qilai Shen/Bloomberg].
The global shipping industry sustained a second cyber attack within a week that's raising concern about disruptions to supply chains already straining to move goods heading into the usual peak season for consumer demand. The International Maritime Organization, a United Nations agency that serves as the industry's regulatory body, said in a statement Thursday it has suffered "a sophisticated cyber attack against the organization's IT systems." A number of IMO web-based services are currently unavailable and the breach is affecting its public website and internal systems, it said. That attack followed the disclosure earlier this week by closely held CMA CGM SA, the world's fourth-biggest container liner by capacity, that its information systems were compromised. The Marseille, France-based company said Thursday that offices are "gradually being reconnected to the network thus improving the bookings' and documentation's processing times." "We suspect a data breach and are doing everything possible to assess its potential volume and nature," the company said in an emailed statement. CMA CGM is among the world's five leading container liners that account for 65% of global capacity, according to Alphaliner data. A rash of cyber incidents has afflicted the shipping industry in recent years, the biggest of which was an intrusion that cost Copenhagen-based A.P. Moller-Maersk A/S about $300 million in 2017. The Maersk incident "has clearly drawn the attention of scammers and cyber criminals who realized that the shipping industry is acutely exposed," said Ken Munro, a security specialist at Pen Test Partners, a cyber-security company with clients in the maritime industry. "If shore-based systems aren't available to book containers, ships can't load and can't generate revenue. Targeted attacks against shipping lines are therefore lucrative for ransomware operators." While it's too soon to say whether the recent attacks will prove to be a brief irritant for global trade or a trigger of wider damage, logistics experts like Bloomberg Intelligence's Lee Klaskow say the cyber threats are a "near-term headwind and headache for sure." The timing of the latest acts of cyber piracy is particularly bad for shipping liners that are still waiting to see some normalcy restored to their seasonal cycles. The pandemic threw supply chains out of sync for everything from paper towels and face masks to trampolines and computer monitors, as consumers were forced to work from home and purchase necessities online.The demand on shippers, which reduced capacity initially in anticipation of deep recessions caused by Covid-19 lockdowns, hasn't really abated because e-commerce purchases have stayed strong and companies are restocking inventories. As a result, the benchmark cost to move cargo containers across the Pacific has tripled since the start of the year.
SOURCE : BLOOMBERG

https://www.aljazeera.com/economy/2020/10/2/cyber-pirates-shipping-body-suffers-second-it-attack-in-a-week
ALJAZEERA *– 02 October 2020*

Alien, il malware che infetta le app Android e svuota i conti correnti delle vittime - Alien è un nuovo trojan bancario per Android individuato dai ricercatori di Threat Fabric che permette di sottrarre le credenziali da numerose app, proponendo all'utente schermate di login fittizie e, quindi, accedendo al dispositivo da remoto per eseguire, come riportato dallo CSIRT Italia, una serie di operazioni:

- registrare le digitazioni da tastiera;
- installare TeamViewer per mantenere l'accesso da remoto al dispositivo;
- raccogliere, inviare o inoltrare SMS;
- sottrarre la lista dei contatti;
- raccogliere dettagli sul dispositivo e la lista delle app;
- registrare dati di geo-localizzazione;
- effettuare richieste USSD;
- inoltrare chiamate;
- installare e avviare altre app;
- aprire il browser e indirizzarlo su pagine specifiche;
- bloccare lo schermo;
- visualizzare le notifiche mostrate sul dispositivo;
- sottrarre codici a due fattori generati da app di autenticazione.

Il **malware** deriva da una sofisticazione rispetto al suo predecessore **Cerberus** che, come malware-as-a-service, ha avuto ultimamente un enorme diffusione e il cui **codice sorgente è stato rilasciato gratuitamente** sui forum underground ed è quindi disponibile per chiunque voglia riutilizzarlo e modificarlo.
Max Heinemeyer, Director of Threat Hunting di Darktrace, lo definisce un malware di "generazione Z" perché prende di mira le app mobili, le comunicazioni sui social media e le cripto valute ed evidenzia come la tipologia di Malware-as-a-Service stia diventando sempre più ambita. Infatti, consente ai criminali di mediocre livello di condurre attacchi informatici altamente professionali. Gli autori di questi attacchi aggiornano costantemente le proprie tecniche e non hanno remore a prendere in prestito parti da strumenti che hanno già avuto una buona riuscita, come Cerberus.
Oggi la stessa minaccia agisce su PC, ma anche sui dispositivi mobili. Nel caso in esame, Alien sfrutta messaggi SMS dannosi o applicazioni mobili fraudolente per divulgare l'infezione.
Gli autori di Alien si sono focalizzati su come eludere l'autenticazione a più fattori, che è una misura di sicurezza sostanziale, ma "non è a prova di proiettile". È necessario ricorrere a tecnologie più performanti, come l'IA, perché, di fronte al fallimento dell'autenticazione a più fattori, si possano prendere decisioni in pochi secondi su una condotta potenzialmente dannosa e neutralizzare la minaccia……..
Il **CSIRT Italiano** per la prevenzione suggerisce download solo da store ufficiali e molta attenzione da parte dell'utente finale per i permessi richiesti dall'app in fase di installazione per individuare richieste fuori luogo, improprie, o troppo "invadenti".
Alien appare come nuovo malware, benché sia la variante di un malware già esistente, quindi per essere sicuri di proteggersi per tempo servono strumenti adeguanti capaci di identificare il codice sorgente comune e classificarlo come malevolo.
https://www.cybersecurity360.it/nuove-minacce/alien-il-malware-che-infetta-le-app-android-e-svuota-i-conti-correnti-delle-vittime/

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

***Cybersecurity360**, Alessia Valentini, 02 ottobre 2020*

PROSSIMI EVENTI

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
Email segreteria@infrastrutturecritiche.it

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

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