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 2021	N. 11/ 2021	Dicembre 2021

Focus on Supply Chain Security: cos'è e come si affronta il rischio

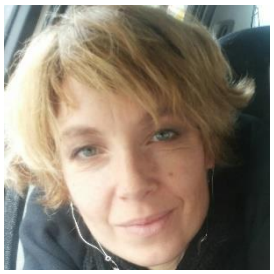
Si chiama Supply Chain 4.0 ed indica la quarta rivoluzione dei sistemi di gestione delle catene di fornitura (supply chain), che integra le operazioni di produzione dell'industry 4.0 con i processi di telecomunicazione e di Information Technology. Oltre agli ovvi obiettivi legati al business, necessari a qualsiasi catena di approvvigionamento (efficienza, tempestività, redditività, interoperabilità) è oggi necessario fronteggiare i rischi operativi digitali e legati alla Cybersecurity.
Lo sviluppo degli attacchi informatici e la protezione da questi è un'area di studio mondiale che procede in parallelo alla adozione pervasiva della digitalizzazione. Le Supply chain 4.0 non sfuggono a questi processi evolutivi e sono quindi sempre più interconnesse e digitalmente abilitate, ma non necessariamente e nativamente resilienti alle minacce informatiche. Anzi i ricercatori che studiano questi temi evidenziano come la catena di approvvigionamento 4.0 abbia una mancanza di standard semantici, scarsa interoperabilità e mancanza di sicurezza nel funzionamento dei processi di produzione e di tecnologia dell'informazione (Fonte Reasearch paper 2020). Quindi i ricercatori evidenziano come ci siano vulnerabilità intrinseche in aggiunta a quelle legate alle tecnologie. Oltre ai prevedibili problemi di digitalizzazione e revisione dei processi fra i fornitori di una catena di approvvigionamento, vi è anche l'integrazione di nuove tecnologie e di interi sistemi digitali: sistemi ERP e gestionali, reti di comunicazione, sistemi integrati abilitanti specifici per settore di mercato, sistemi cyber-fisici, Internet of Things e Industrial Internet of Things ma anche applicazioni di intelligenza artificiale, blockchain, contratti intelligenti. Il rischio di sicurezza legato alla supply chain è quindi un mix di valutazioni di rischio legate non solo all'intero processo visto come un unicum, ma anche legato al singolo sistema digitale coinvolto, con implicazioni sulla tecnologia presa da sola e nelle combinazioni con le altre. Il rischio della catena di approvvigionamento è definito come l'improvvisa probabilità di un attacco informatico che influisca sul livello macro o micro dei processi della catena di approvvigionamento e che porti all'impatto in qualsiasi parte delle operazioni della catena di approvvigionamento incluse le componenti di IT e OT. Si tratta dunque di un sistema complesso di cui garantire la sicurezza informatica a vari livelli di granularità (Fonte Reasearch paper 2020).
Secondo Daniel Stanton autore del libro "Supply Chain Risk Management for dummies", un sistema di gestione del rischio della catena di approvvigionamento (SCRM) fornisce visibilità per mantenere la catena di approvvigionamento operativa in qualsiasi condizione di mercato o nei casi di un attacco informatico. Un sistema SCRM può contribuire ad evitare rischi prevenibili non solo vagliando e monitorando attentamente i fornitori, ma anche identificando tutte le minacce lungo la catena di approvvigionamento e fornendo i mezzi per collaborare con i partner e mitigare il rischio. Per impostarlo correttamente Daniel Stanton suggerisce un approccio (ispirato allo standard NIST CF n.d.r.) basato sui seguenti passi:

1. **Stabilire le priorità:** l primo passo nella costruzione di un processo di gestione del rischio di Supply Chain è determinare quali parti della catena di fornitura saranno incluse. Idealmente, si dovrebbero coprire tutti i prodotti e servizi acquistati dall'azienda e tutti i fornitori, ma molte aziende inizialmente danno la priorità a un sottoinsieme della loro base di fornitura totale, in particolare quelle aree che sono più critiche per la produzione.

2. **Identificare e mappare tutte le componenti della supply chain per la tenuta sotto controllo:** Un buon punto di partenza è creare un elenco di oggetti a rischio come, ad esempio, infrastrutture di trasporto o dotazioni particolari per le quali il fornitore è prioritario nella catena di fornitura. I fornitori si distinguono fra primari, secondari etc, quindi idealmente, un processo efficace di gestione del rischio della catena di approvvigionamento dovrebbe identificare gli oggetti di rischio ai diversi livelli in una catena di approvvigionamento.
3. **Identificare i rischi specifici:** per ogni fornitore mappato è necessario identificare i rischi che potrebbero avere un impatto su di lui, creando un profilo di rischio specifico costituito dalla valutazione percentuale e dalla valutazione di impatto di ogni voce.
4. **Introdurre misure di protezione per ridurre i rischi:** per ogni voce della lista di cui al punto precedente è appropriato prevedere misure di protezione perché la mitigazione è la chiave per diventare proattivi nella gestione del rischio. È necessario anche condividere con i fornitori l'approccio seguito, anche per avere contezza della reale implementazione delle misure di protezione. Di recente anche per le catene di approvvigionamento si stanno adottando approcci di "Zero trust" security in cui si richiede la verifica, l'autenticazione e l'approvazione per l'accesso di tutte le risorse: account utente, applicazioni e sistemi. Anche gli utenti all'interno di una determinata infrastruttura tecnologica devono confermare i propri dati ogni volta che richiedono l'accesso a qualsiasi risorsa interna o esterna alla rete. Questi controlli zero trust dovrebbero essere estesi anche per tutte le aziende della stessa supply chain in modo che un attaccante non possa intrufolarsi. (per approfondimenti sui motivi di adozione dell'approccio zero trust nella supply chain si suggerisce la lettura delle indicazioni edite dal WEC)
5. **Monitorare i rischi e definire degli indicatori:** per avere una chiara e dinamica visibilità dei rischi si rende necessario introdurre indicatori scelti in funzione della loro capacità di indicare una situazione di variazione del rischio per gestire la possibile evoluzione.
6. **Introdurre mezzi di individuazione delle situazioni di rischio (incidente informatico)**: per capire che qualcosa di grave sta avvenendo è necessario decidere come gli indicatori per attivare l'azione di emergenza. Si inizia individuando i valori di soglia e definendo le condizioni per l'attivazione di una risposta al rischio.
7. **Personalizzare le attività di mitigazione e response:** secondo il comportamento degli indicatori si possono attuare misure di mitigazione e azioni di response attivando i gruppi di sicurezza preposti o i fornitori che si occupano di incident handling in outsourcing. In ogni caso il risultato deve portare ad una azione di contenimento, riduzione di impatto e progressiva normalizzazione della operatività della catena di approvvigionamento fino al ripristino della situazione pre-incidente di sicurezza.
8. **Introduzione della automazione del sistema di gestione:** per effettuare attività in automatico si ricorre a sistemi di Machine learning che possano automatizzare le decisioni in funzione di determinate casistiche. È ovviamente cruciale condividere i sistemi di "apprendimento e risposta" (Machine learning, automation &response) anche con i fornitori perché possano essere attuati correttivi lungo tutta la catena di fornitura. In questi casi non è affatto scontato che tutte le terze parti acconsentano ad una gestione che sembrerebbe sfuggire al loro controllo diretto. Le implicazioni sono molteplici (alterazione degli SLA di fornitura, penali) e necessitano di accordi contrattuali integrativi per la gestione di ogni evenienza.

Un sistema digitale di supply chain ha un valore che deriva dalla capitalizzazione delle opportunità di business e dalla riduzione al minimo dei rischi legati alla sicurezza informatica. Infatti, i singoli fornitori contribuiscono a generare valore che alla fine del processo di supply chain porta a un vantaggio competitivo, ma tutto ciò resta vero se e solo se i rischi di sicurezza informatica, lungo tutta la filiera

sono individuati, monitorati gestiti e mitigati al fine di mantenere alta l'operatività eventualmente anche in caso di attacco. Per impostare un business case di supply chain security e condividerlo con i fornitori motivandoli ad affrontare una valutazione dei rischi di filiera, è opportuno mostrare il ROI dell'iniziativa in termini di benefici nella diminuzione degli impatti potenziali, verso i costi di investimento per le dotazioni e l'impostazione del processo di tenuta sotto controllo dei rischi.
Qualora si voglia approfondire la modalità per avviare un processo di supply chain security ispirandosi a casi reali si può consultare il sito di GOV.UK che ha pubblicato linee guida ed esempi specifici per procedere nella messa in sicurezza delle catene di approvvigionamento come uno degli ambiti della più ampio obiettivo di Cyber resilience per le organizzazioni commerciali.
(Riprodotto da ISACA Rome Chapter Nwesletter)



Alessia Valentini
Consulente di Cybersecurity, Advisor e Giornalista. Attualmente in Gruppo Daman svolge attività di Advisor, Business Developer e Consulente di Cybersecurity. Fa parte delle "Women for Security" la community di Cyberladies nata nell'ambito del Clusit. È Giornalista presso l'ODG del Lazio dal 2013. Ha conseguito la certificazione CISA /ISACA nel 2017. È stata consigliere direttivo in Afcea (Armed Forces Electronic Association) dal 2014 al 2016

ATTIVITA' DELL'ASSOCIAZIONE

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.

NUOVO SITO WEB AIIC

Ricordiamo che è ormai 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.
Potete scriverci al nostro solito indirizzo 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

GRUPPI DI LAVORO AIIC

Sono in fase avanzata di lavoro i due Gruppi di Lavoro AIIC su "Disciplina normativa della criticità" coordinato da Luisa Franchina e su "Protezione degli spazi pubblici" coordinato da Sandro Bologna. I risultati, che verranno esposti in due apposite pubblicazioni, verranno presentati ai soci in occasione dei prossimi incontri, in presenza o on-line.

NEWS E AVVENIMENTI

Infrastructure bill includes $1.9 billion for cybersecurity

Passage of the infrastructure bill includes $1.9 billion for cybersecurity, and more could be on the way with the Build Back Better and other bills working their way through Congress. On Friday, Congress passed one of President Biden's signature pieces of legislation, the $1 trillion Infrastructure Investment and Jobs Act. This landmark bill promises not only massive upgrades to the nation's aging infrastructure but also boosts government cybersecurity spending by $1.9 billion. Among its provisions is a new $1 billion grant program to help state, local, tribal and territorial governments protect themselves from malicious actors and modernize systems to protect sensitive data, information, and public critical infrastructure. The Federal Emergency Management Agency (FEMA), which runs the Department of Homeland Security's (DHS's) existing grant programs, will provide the funds over four years starting in fiscal year 2022, with the Cybersecurity and Infrastructure Security Agency (CISA) serving as a subject matter expert.

The bill also incorporates the Cyber Response and Recovery Act of 2021, which authorizes $100 million over five years to help the government quickly respond to cybersecurity intrusions. Another notable

provision is $21 million in funding for the newly created office of the National Cyber Director (NCD) to hire qualified personnel to support its essential cybersecurity mission. The bill further requires the Environmental Protection Agency (EPA) and CISA to identify public water systems that, if degraded or rendered inoperable due to a cyber-attack, would lead to significant impacts on the health and safety of the public. (continua…)
https://www.csoonline.com/article/3639019/whats-next-in-congress-for-cybersecurity-after-enactment-of-the-infrastructure-bill.html
CSOONLINE *-Cynthia Brumfield - NOV 8, 2021*

La gestione dei rischi ransomware: ecco le best practice suggerite dal NIST - Il National Institute of Standards and Technology (NIST) ha pubblicato una nuova revisione della bozza di guida per le organizzazioni sugli attacchi ransomware. Vediamo come può essere utilizzata per contrastare queste pericolosissime e sempre più frequenti minacce.
Abbiamo imparato che il ransomware, fra le tipologie di malware, è fra i più pericolosi di sempre: una minaccia molto seria, tanto che anche il NIST, il National Institute of Standards and Technology, ha addirittura codificato un apposito "Profile" del suo famoso Cybersecurity Framework per aiutare le organizzazioni nella gestione dei rischi. Un documento, quello del NIST, che incrementa ulteriormente le pubblicazioni sui ransomware. Ricordiamo, tra tutte:
la NIST Special Publication 1800-11 – Data Integrity Recovering from Ransomware and Other Destructive Events;
la NIST SP 1800-25 – Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events;
la NIST Special Publication (SP) 1800-26 – Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events.
Indice degli argomenti
Il contenuto del documento del NIST
La gestione dei rischi ransomware
La gestione dei rischi ransomware: best practice
Conclusioni
(continua)
https://www.cybersecurity360.it/nuove-minacce/la-gestione-dei-rischi-ransomware-ecco-le-best-practice-suggerite-dal-nist/
CYBERSECURITY360 *- Stefano Posti - 10 Nov 2021*

Costi della sicurezza per l'attuazione delle misure anti-COVID nei cantieri - Nell'articolo che segue vengono fornite indicazioni utili sulla valutazione dei costi per l'attuazione delle misure finalizzate a prevenire la trasmissione del COVID-19 nei cantieri temporanei e mobili come da D. Lgs. 81/08 e s.m.i.: le misure di sicurezza richieste nel Protocollo anti-contagio nei cantieri, i provvedimenti della Regione Piemonte, la determinazione dei costi di sicurezza non soggetti a ribasso e degli oneri di sicurezza aziendali, i criteri per una corretta valutazione del quadro economico dei nuovi appalti.
(continua)
https://www.ingenio-web.it/32695-costi-della-sicurezza-per-lattuazione-delle-misure-anti-covid-nei-cantieri
INGENIO *- Giberti Luca Stefano - 24/11/2021*

L'IoT cresce, ma meno del previsto. I risultati del Rapporto McKinsey - Rispetto al precedente studio del 2015, il mercato è cresciuto molto, ma non così velocemente come ci si aspettava. Il settore ha dovuto affrontare i venti contrari rappresentati da gestione del cambiamento, costi, talenti e sicurezza informatica, in particolare nelle imprese.
Nel mese di novembre 2021, McKinsey & Co. ha pubblicato un voluminoso report dal titolo "The Internet of Things Catching up to an accelerating opportunity". Ne abbiamo estratto i punti salienti che tracciano un profilo molto interessante di quale sarà il futuro dell'IoT.
Nel 2015, il McKinsey Global Institute ha pubblicato un rapporto di ricerca intitolato The Internet of Things: Mapping the value beyond the hype. Il report ha analizzato il potenziale economico che l'IoT potrebbe liberare attraverso la considerazione di centinaia di casi d'uso nelle impostazioni fisiche in cui potrebbero essere implementati. Sei anni dopo, in un nuovo rapporto, The Internet of Things: Catching up to an accelerating opportunity, l'analisi è stata aggiornata per stimare quanto di quel valore è stato raccolto, come il valore potenziale dell'IoT potrebbe evolversi nel prossimo decennio e i fattori che spiegano entrambi.
Il mercato è cresciuto considerevolmente negli anni successivi al 2015, ma non così velocemente come ci si aspettava. L'IoT ha affrontato venti contrari legati alla gestione del cambiamento, ai costi, ai talenti e alla sicurezza informatica, in particolare nelle imprese.
Ecco cosa emerge dall'ultima ricerca McKinsey.
Indice degli argomenti
Un potenziale valore economico in crescita
In che modo la pandemia di COVID-19 ha influenzato il mercato IoT
Outlook per IoT nell'industria
Le prospettive per l'IoT
Salute e benessere
Automotive
Domotica
Mercato IoT, la ripartizione geografica
IoT: punti a favore e punti contrari
Conclusioni
(continua)
https://www.internet4things.it/iot-library/esperti-e-analisti/liot-cresce-ma-meno-del-previsto-i-risultati-del-rapporto-mckinsey/
Internet4things *- Pierluigi Sandonnini - 26 Novembre 2021*

Cosa prevede il decreto minicodice sulla progettazione antincendio nei luoghi di lavoro - Ad ottobre del prossimo anno entrerà in vigore il "decreto minicodice" che 'manderà in pensione' lo storico D.M. del 10 marzo 1998 sui "Criteri Generali di sicurezza antincendio". Ecco un approfondimento sul tema.
La genesi del "Decreto minicodice"
Sulla Gazzetta Ufficiale n. 259 del 29 ottobre 2021 è stato finalmente pubblicato il Decreto del Ministro dell'Interno, di concerto con il Ministro del Lavoro e delle Politiche Sociali 3 settembre 2021 recante "Criteri generali di progettazione, realizzazione ed esercizio della sicurezza antincendio per luoghi di lavoro, ai sensi dell'articolo 46, comma 3, lettera a), punti 1 e 2, del Decreto Legislativo 9 aprile 2008, n. 81".
Il D.M. 3 settembre 2021, detto anche "Decreto minicodice" è di fondamentale importanza, anche perché dal 29 ottobre 2022, con la sua entrata in vigore, ad un anno dalla pubblicazione, verrà definitivamente

abrogato il D.M. 10 marzo 1998, "Criteri generali di sicurezza antincendio e per la gestione dell'emergenza nei luoghi di lavoro" decreto storico, che ha segnato un'epoca: la seconda rivoluzione della prevenzione incendi, l'età di mezzo.
(continua)
https://www.ingenio-web.it/32796-cosa-prevede-il-decreto-minicodice-sulla-progettazione-antincendio-nei-luoghi-di-lavoro
***INGENIO** - Vanzini Vasco - 01/12/2021*

I grossi rischi cyber delle utility italiane: ecco le sfide Un bersaglio sensibile, facile e conveniente. Ecco perché le utility sono sempre più nel mirino degli attacchi informatici. Ma come si pongono le utility italiane nella sfida della cybersecurity? Molto è stato fatto, ma non è ancora sufficiente. Servono più investimenti, consapevolezza e formazione
Il radicamento sul territorio e la pervasività dei servizi, dalla fornitura di energia elettrica e gas, al ciclo idrico, alla gestione dei rifiuti, rendono le utility un fattore essenziale per la qualità della vita e per tutte le attività economiche.
Queste caratteristiche, tuttavia, rendono anche queste imprese molto articolate e complesse con **elementi di fragilità** in un mondo sempre più interconnesso e soggetto ad attacchi informatici. La resilienza delle infrastrutture delle utility diventa quindi sempre più importante a fronte sia di **eventi climatici** estremi crescenti che di **vulnerabilità connesse allo sviluppo della digitalizzazione**.
Ed è un problema grave, considerando che il settore delle **public utility** costituisce un asse portante del sistema socio-economico di ogni nazione, contribuendo con infrastrutture e servizi alla crescita, alla sostenibilità ambientale e al progresso sociale, portando benefici ai cittadini e creando valore per le imprese.
Indice degli argomenti

- Le ragioni dietro gli attacchi alle utility
- I tre motivi dell'escalation di attacchi alle utility
- Le utility italiane nella sfida della cybersecurity
    - La correlazione tra dimensioni e numero di attacchi registrati
    - La ripartizione degli attacchi su base territoriale
- Quanto sanno difendersi le utility italiane?
- Quanto investono le utility italiane in sicurezza informatica?
- Conclusioni

Le ragioni dietro gli attacchi alle utility
Sebbene non sia visibile, in ogni momento la rete è, infatti, attraversata da innumerevoli attacchi informatici. Attacchi provenienti da qualsiasi parte del mondo, capaci di colpire qualsiasi altra parte del mondo. Basta dare un'occhiata alle numerose mappe liberamente disponibili su Internet che tracciano in tempo reale i tentativi di attacco per rendersi conto di come il mondo digitale sia diventato un immenso campo di battaglia. Le ragioni dietro gli attacchi informatici sono **innumerevoli**. In alcuni casi, lo scopo è meramente estorsivo: sono i cosiddetti attacchi ransomware, che paralizzano un sistema per ottenere il pagamento di un **riscatto**, o i **data theft**, che trafugano informazioni sensibili da rivendere al miglior offerente. In altri, invece, c'è una componente politica, economica o addirittura ideologica: parti politicamente avverse, competitor industriali o anche attivisti (i cosiddetti hacktivist, crasi di hacker e activist) possono avere interesse nel danneggiare un'azienda o uno Stato.
In questo grande campo di battaglia che è il mondo digitale, le utility si trovano in una posizione molto delicata e sono **prede ambite del cybercrime**. (continua….)

https://www.agendadigitale.eu/sicurezza/cybersecurity-quanto-e-perche-sono-a-rischio-le-utility-italiane-sfide-e-scenari/
Agendadigitale *- Alessandro Marangoni* ***-*** *03 Dic 2021*

La sicurezza informatica delle istituzioni pubbliche per la resilienza del sistema paese - È cresciuta la consapevolezza della centralità delle infrastrutture informatiche e della loro difesa per la resilienza del paese. Grazie alle risorse dedicate alla sicurezza dal PNRR e alla recente creazione dell'Agenzia per la sicurezza nazionale cibernetica ci sono le condizioni per definire e mettere in atto una nuova strategia di protezione coordinata per tutte le amministrazioni. L'opinione di alcune realtà pubbliche e private.
La digitalizzazione a tappe forzate su impulso della pandemia ha aumentato la superficie di attacco e ha moltiplicato l'attivismo del cybercrime soprattutto verso amministrazioni pubbliche e sanità, come hanno evidenziato diverse testimonianze in occasione del Forum Pa 2021. È però cresciuta al contempo la consapevolezza della centralità delle infrastrutture informatiche e della loro difesa per la resilienza del paese. Grazie alle risorse dedicate alla sicurezza dal PNRR e alla recente creazione dell'Agenzia per la sicurezza nazionale cibernetica ci sono le condizioni per definire e mettere in atto una nuova strategia di protezione coordinata per tutte le amministrazioni

"La pandemia ha evidenziato che la sfera cibernetica è un asset fondamentale della vita politica ed economica delle democrazie evolute". Se si concorda con questa dichiarazione di Ivano Gabrielli, Direttore della III Divisione del Servizio Polizia Postale e delle Comunicazioni, l'immediata conseguenza è garantire la sicurezza informatica per le amministrazioni pubbliche come condizione per la resilienza del Paese. "Inevitabile immaginare sistemi organizzativi nella Pa che mettano al centro il tema della sicurezza informatica finora marginalizzata rispetto alla conduzione di sistemi operativi e all'erogazione di applicativi", aggiunge Gabrielli che evidenzia come nell'ultimo anno siano aumentati del 130% gli attacchi informatici rilevati dal centro della Polizia Postate e del 230% i reati contro le persone commessi tramite rete.
La pandemia ha giocato un ruolo importante diretto e indiretto. Lo ricorda Priscilla Inzerilli, membro dell'Associazione Italiana Esperti in Infrastrutture Critiche, evidenziando che il Covid è stato il cavallo di troia per il 90% dei messaggi spam e fishing che hanno avuto come target soprattutto singoli e lavoratori in smart working in condizioni di scarsa sicurezza. L'Italia si è posizionata al terzo posto per numero di attacchi informatici con quasi 5 milioni di malware rilevati con target principale il settore pubblico, seguito dal bancario, dalla produzione industriale e dal settore sanitario. "Questo posizionamento può avere anche una valenza positiva: indica infatti un elevato numero di detection, la capacità di comunicazione degli eventi e dell'implementazione delle misure di sicurezza", sottolinea Inzerilli.
Secondo una ricerca Vmware, rivolta a Cio e Ciso, a cui fa riferimento Rodolfo Rotondo, Business Solution Strategist Director dell'azienda, la quasi totalità delle aziende italiane ha subito almeno un attacco, l'83% con esito negativo sulla reputazione e un terzo con danni finanziari, realizzata. A livello globale si stima danno da cyber crime di 6mila miliardi di dollari in crescita.
Indice degli argomenti
Quali priorità di investimento?
Collaborazione è la parola chiave per affrontare le sfide della sicurezza
(continua)
https://www.zerounoweb.it/cio-innovation/la-sicurezza-informatica-delle-istituzioni-pubbliche-per-la-resilienza-del-sistema-paese-2/

Zerounoweb *- Elisabetta Bevilacqua - 06 Dic 2021*

"Hello Quantum World:" New cybersecurity service uses entanglement to generate cryptographic keys" The new service protects against current and future cyberattacks, according to Quantinuum CEO, and works with existing cybersecurity systems.
Quantinuum is the new company that combines trapped ion hardware from Honeywell Quantum Solutions and open-source software from Cambridge Quantum to create a full-stack quantum computing company. Quantinumm's software company Cambridge Quantum announced a new way to provide cryptographic keys that uses Honeywell's H1, entanglement and an API. Quantum Origin can run on any quantum computer and is designed to integrate into existing cybersecurity solutions. This new cloud-based method uses quantum entanglement to generate cryptographic keys and is based on verifiable quantum randomness, according to the company. The company generates the keys before encrypting them with a transport key and relaying them back to a customer. Duncan Jones, head of cybersecurity at Cambridge Quantum, said Quantum Origin is kickstarting the quantum cybersecurity industry. "We can isolate the particular bit of quantum behaviour we are looking for and then make it available to other systems so that everyone can benefit and security can be increased across the board," he said. **Quantinuum shifts conversation from counting qubits to perfecting cybersecurity solution.** Ilyas Khan, CEO of Quantinuum and founder of Cambridge Quantum, said that the key generator was tested on Oxford Quantum's and IBM's quantum computers.
"At the moment, the best results have come from a trapped ion system but that could change tomorrow," he said. "The product is platform agnostic and could generate the key using any number of quantum computers that come online in the future."
Jones said that Cambridge Quantum's device-agnostic approach is what makes this service different from other attempts to use quantum computers for cybersecurity.
In a white paper about Quantum Origin, Cambridge Quantum describes device independence this way: "In a fully device-independent (DI) protocol, only minimal assumptions are made about the physical device that executes the protocol. Instead, the device is treated as a black box, and the protocol simply provides inputs and interrogates the output from the device."
The product supports RSA and AES algorithms as well as the post-quantum cryptography algorithms being standardized by the National Institute for Standards and Technology. The service is priced per key generated for customers. (continua….)
https://www.techrepublic.com/article/hello-quantum-world-new-cybersecurity-service-uses-entanglement-to-generate-cryptographic-keys/
Techrepublic*- Veronica Combs - December 7, 2021*

Ispezione, rilievo, manutenzione, digitalizzazione e monitoraggio in esercizio delle infrastrutture strategiche - Nella splendida cornice dell'Aula biblioteca del Centro Congressi dell'Hotel Villa Maria Regina di Roma, il 25 novembre 2021 si è tenuto il convegno tecnico dal titolo "Ispezione, rilievo, manutenzione, digitalizzazione e monitoraggio in esercizio delle infrastrutture strategiche" organizzato dall'Associazione scientifico-culturale MASTER in collaborazione con l'Ordine degli Ingegneri della Provincia di Roma e la Fondazione dell'Ordine degli Ingegneri di Roma.
Infrastrutture, come mantenerle in sicurezza?
In Italia abbiamo circa 840.000 km di strade di cui 8.006 km di autostrade e 27.259 km strade statali (ANAS) con 2.179 gallerie, 21.072 ponti e viadotti e 6.320 cavalcavia.

A questi si aggiungono 17.530 km di ferrovie nazionali e regionali con 18.847 ponti, viadotti e gallerie; 1.130 km di ferrovie isolate con 1.529 ponti, viadotti e gallerie e 225 km di impianti di trasporto rapido di massa (metropolitane), di cui 131,6 km in galleria, dislocati in sette città.
I soggetti, tra gestori delle infrastrutture, imprese esercenti il servizio e centri di formazione, sono più di 8.000.
Questi sono alcuni dei numeri dell'immenso patrimonio nazionale ed è evidente che è impossibile parlare di infrastrutture senza occuparsi contemporaneamente di sicurezza, di cultura della conservazione e di manutenzione delle opere esistenti, che soffrono sia la condizione di obsolescenza sia l'assenza di un sistema di monitoraggio in esercizio.
Lo sviluppo normativo in merito alla sicurezza delle infrastrutture civili è stato il motore di una forte spinta all'innovazione tecnologica e oggi i professionisti del settore hanno a disposizione strumenti e tecnologie sempre più all'avanguardia in grado di monitorare lo stato di salute di un'opera e che consentono di programmare interventi mirati di manutenzione e conservazione della stessa.
(continua)
https://www.ingenio-web.it/32496-ispezione-rilievo-manutenzione-digitalizzazione-e-monitoraggio-in-esercizio-delle-infrastrutture-strategiche
***INGENIO** - MASTER - Associazione Materials and Structures, Testing and Research - 07/12/2021*

Bosses are reluctant to spend money on cybersecurity. Then they get hacked .Preventing a cyberattack is more cost effective than reacting to one - but many boardrooms still aren't willing to free up budget. Many businesses still aren't willing to spend money on cybersecurity because they view it as an additional cost – and then find they have to spend much more cash recovering from a cyber incident after they get hacked. Cyberattacks like ransomware, business email compromise (BEC) scams and data breaches are some of the key issues businesses are facing today, but despite the number of high-profile incidents and their expensive fallout, many boardrooms are still reluctant to free up budget to invest in the cybersecurity measures necessary to avoid becoming the next victim.
The cost of falling victim to a major cyber incident like a ransomware attack can be many times more than the cost of investing in the people and procedures that can stop incidents in the first place – something many organisations only fully realise after it's too late.
"Organisations don't like spending money on preventative stuff. They don't want to overspend, so a lot of organisations will sort of be penny-wise and pound-foolish kind of places where they wait for the event to happen, and then they have the big expense of cleaning it up," Chris Wysopal, co-founder and CTO of cybersecurity company Veracode, told
It's then that they realise that they could have spent less if they had prevented the attack, he said: "A lot of organisations are going through that right now".
For example, an organisation might end up paying millions of dollars to ransomware criminals for the decryption key for an encrypted network – then there's the additional costs associated with investigating, remediating and restoring the IT infrastructure of the whole business after the incident.
"Just the ransoms that organisations are paying, if they don't have cyber insurance, could certainly pay for a lot of cybersecurity professionals. And cyber-insurance rates are going up, so it's getting more expensive across the board for organisations because of the threat," said Wysopal.
Even for organisations that do have a fully fledged cybersecurity strategy, training, hiring and retaining staff can still pose a challenge because of the high demand for employees with the required skills. (continua…)
https://www.zdnet.com/article/too-many-bosses-are-reluctant-to-spend-money-on-cybersecurity-then-they-get-hacked/

ZDENET - *Danny Palmer* **-** *December 7, 2021*

Log4Shell, allarme rosso dell'Agenzia cyber. Tutti i dettagli. *Si chiama Log4Shell, è una vulnerabilità zero-day che da giorni mette in allerta big tech e governi di mezzo mondo. L'Agenzia per la cybersicurezza nazionale (Acn) guidata da Roberto Baldoni scende in campo per mitigare i rischi. Ecco l'allarme e tutti i dettagli.* Un primo banco di prova per l'Agenzia per la cybersicurezza nazionale guidata da **Roberto Baldoni**. Si chiama Log4Shell ed è una vulnerabilità critica che in queste ore sta mettendo in allerta big tech e governi. Attacca il modulo open source di Apache Project, cuore della maggior parte delle applicazioni ospitate dai server di tutto il mondo, e può innescare un pericoloso effetto a catena. A lanciare l'allarme in Italia è l'Acn con un comunicato che invita alla prudenza e parla di "una vasta e diversificata superficie di attacco sulla totalità della rete internet". "I tecnici dell'Agenzia per la Cybersicurezza Nazionale, in costante contatto con le omologhe agenzie europee ed internazionali, raccomandano, vista la pericolosità della vulnerabilità, di ridurre al minimo la sua esposizione su internet applicando le necessarie misure ai propri server nel più breve tempo possibile", si legge nella nota diffusa questo pomeriggio. Scoperta già il 24 novembre dal colosso cinese Alibaba, la vulnerabilità riguarda una utility open source di Java utilizzata da migliaia di aziende per effettuare debug e logging all'interno di più portali e servizi web. In una nota anche l'Agenzia cyber degli Stati Uniti (Cisa) ha suonato un campanello d'allarme: "Un aggressore da remoto potrebbe sfruttare questa vulnerabilità per prendere il controllo di un sistema infetto". Tra i principali target della vulnerabilità c'è Minecraft: proprio dagli utenti di siti legati al popolare gioco online sono partite le prime segnalazioni. "La sua semplicità di sfruttamento, anche da parte di attori non sofisticati, rende la segnalata vulnerabilità particolarmente grave", spiegano dall'Acn. Per l'Agenzia si tratta del primo test di intervento da quando è stata inaugurata. Assicurare la continuità di un servizio essenziale non è una prova banale, per un'organizzazione che è ancora in piena fase di start-up e al momento conta appena 90 risorse. Sul sito dello Csirt (Computer security incident response team) sono stati intanto pubblicati nuovi dettagli sulla vulnerabilità definita "di livello critico", cui è stato assegnato il massimo punteggio (CVSSv3: 10) perché "permette l'esecuzione di codice da remoto (RCE) senza autenticazione"."L'eventuale sfruttamento della falla consente l'esecuzione di codice arbitrario a danno dell'applicazione affetta", avvisano dallo Csirt. "Gli aggressori, che non necessitano di un accesso preventivo al sistema, possono inviare una richiesta https malformata tramite una stringa appositamente predisposta, per generare un log su Log4j – che adotta JNDI (Java Naming and Directory Interface) – al fine di registrare la stringa dannosa nel registro dell'applicazione".Di qui il funzionamento di Log4Shell. (continua….)
https://formiche.net/2021/12/log4shell-allarme-cyber-hacker/
Formiche - *Francesco Bechis - 12/12/2021 –*

Cybersecurity, i rischi di 5G e IoT per le smart factory: il ruolo delle telco e gli scenari La crescita esponenziale di dispositivi IoT collegati alle reti degli operatori tlc e alle infrastrutture cloud, procedono di pari passo con lo sviluppo delle reti 5G necessarie per la loro diffusione. Questo scenario sta creando un ambiente ricco di insidie di cybersecurity, specie con l'evoluzione verso la smart factory
Il **5G** sarà al centro di una nuova rivoluzione industriale che porterà alla nascita di servizi che cambieranno il modo di vivere, produrre, lavorare e muoversi delle persone. Questo è il motivo per cui è essenziale e urgente rafforzare le norme di sicurezza esistenti in questo settore. La nuova architettura della rete 5G presenta infatti **innegabili vantaggi** ma introduce nuovi tipi di minacce alla sicurezza

poiché crea una superficie d'attacco aumentata. Questo impatta sul **perimetro di sicurezza nazionale**. In caso di "rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi", l'art. 5 del **Perimetro di Sicurezza Nazionale Cibernetica** concede al Presidente del Consiglio dei ministri il potere di disattivare, in modo parziale o totale, uno o più apparati o prodotti impiegati nelle reti e nei sistemi colpiti. **Tutte le aziende, anche le PMI, devono quindi considerare la sicurezza informatica come parte integrante delle loro strategie di trasformazione digitale**. Non solo, infatti, gli attacchi informatici sono pericolosi in quanto espongono al furto di dati riservati, spesso non denunciati, ma sono costosi in termini di tempo e risorse per superare gli attacchi con danni permanenti. Proteggendo i propri asset informatici e i dati, le organizzazioni possono concentrarsi sull'innovazione e sul business restando così operative. Dare priorità alla sicurezza informatica, specie con l'evoluzione verso la smart factory, è una parte fondamentale della trasformazione digitale per avere **sistemi di business resilienti**. Servono le competenze e gli investimenti per non farsi cogliere impreparati ed essere competitivi.

Indice degli argomenti

- Lo scenario di sicurezza cibernetica tra 5G e IoT
- Attacchi DDOS verso le PMI: il report ENISA
- Il ruolo delle infrastrutture di telecomunicazioni nella digital transformation
- Le competenze per prepararsi alle sfide cyber del 5G

Lo scenario di sicurezza cibernetica tra 5G e IoT

Lo scenario di sicurezza cibernetica si complica ulteriormente con l'utilizzo dell'IOT massivo (Internet of Things) abilitato dal 5G in ambito sanitario, mobilità, Smart City e Industria 4.0 in tempo di Covid. Verranno evidenziati alcuni scenari di cyber security legati all'evoluzione delle infrastrutture TLC e come sia possibile mitigare i rischi legati alla evoluzione dello Smart Working e della Smart Factory imposti dai cambiamenti (continua….)

https://www.agendadigitale.eu/sicurezza/cybersecurity-i-rischi-di-5g-e-iot-per-le-smart-factory-il-ruolo-delle-telco-e-gli-scenari/

AgendaDigitale *- Giovanni Gasbarrone* ***-*** *13 dice 2021*

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

AIIC

augura a tutti

Buone Feste e Arrivederci al 2022

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link

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

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

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.