sanitainformazione.it
www.sanitainformazione.it
Utenti unici: 762

Rassegna del 09/09/2021
Notizia del: 08/09/2021
Foglio:1/2

LAVORO | 8 Settembre 2021 15:05

Cybersicurezza, Nicora (FIASO): «Urgente investire in "immunità di gregge" dei sistemi informativi sanitari»

Il vicepresidente FIASO: «Smartworking e telemedicina sono nuove porte a diposizione degli hacker. Per garantire più sicurezza investire in formazione. Dotare i device sanitari di certificato che ne attesti il grado di cybersecurity».

di Isabella Faggiano

Criptano i dati informatici e sono disposti a decriptarli solo dietro pagamento di un riscatto. O, ancora, se ne impossessano per poi rivenderli a caro prezzo. È così che gli hacker incrementano il loro business illegale. Un giro illecito che ora ha allungato i suoi tentacoli anche sul Sistema Sanitario Nazionale. «Il ripetersi di episodi di violazione della sicurezza informatica del SSN, come gli attacchi hacker ai server dell'Agenzia regionale di Sanità della Toscana e della Regione Lazio, è un campanello d'allarme», dice **Carlo Nicora**, vicepresidente della Federazione Italiana delle Aziende Sanitarie ed Ospedaliere (FIASO) e Direttore generale della Fondazione IRCCS Policlinico San Matteo di Pavia. «Un avvertimento da non trascurare soprattutto ora che, attraverso il PNRR, la digitalizzazione del comparto sanità subirà una decisiva accelerata», aggiunge.

L'impegno di FIASO

L'interesse dalle FIASO alla cybersicurezza non è una novità: si è dedicata, con costanza, nel corso degli anni, ad attività di rafforzamento della prevenzione dei fattori di rischio, collaborando anche con l'AGID (l'Agenzia per l'Italia Digitale) e la Polizia postale. «Per i sistemi informativi della Sanità pubblica è necessaria "un'immunità di gregge" – sottolinea Nicora -. Finora ci siamo sempre dedicati a progettarne la struttura, garantendo, attraverso appositi backup, la duplicazione dei dati». Attualmente, alla luce dell"interesse che gli hacker hanno mostrato per il SSN è necessario occuparsi anche della loro sicurezza, scongiurando ulteriori pericoli.

GLI ARTICOLI PIU' LETTI

NON CATEGORIZZATO
Covid-19 e vaccini: i numeri in Italia e nel mondo
Al 9 settembre, sono 222.568.068 i casi di Covid-19 in tutto il mondo e 4.596.463 i decessi. Ad oggi, oltre 5,56 miliardi di dosi di vaccino sono state somministrate nel mondo. Mappa elaborata dalla&n...
di Redazione

SALUTE
Aumentano i contagi tra i sanitari: 600% in più in un mese, l'84% sono infermieri
La presidente FNOPI Mangiacavalli interpreta i dati dell'ISS. Anche nel Regno Unito gli studi confermano che la protezione dall'infezione si riduce dopo 5 mesi dalla seconda dose per Pfizer e AstraZen...
di Redazione

COVID-19, CHE FARE SE...?
Chi ha diritto alla certificazione di esenzione dal vaccino anti Covid-19?
Il vademecum della SIMG, in collaborazione con ministero della Salute e Istituto Superiore di Sanità, sui casi particolari in cui la vaccinazione contro il Covid-19 è controindicata o ri...
di Redazione

RUBRICHE

MINISTERO
A scuola in sicurezza: distanziamento, mascherine e test salivari. Ma cosa fare se c'è un positivo?

ASSICURAZIONI
La polizza di responsabilità civile sanitaria garantisce soltanto nei casi di danno fisico?

SANITÀ INTERNAZIONALE
Israele potrebbe raggiungere

sanitainformazione.it
www.sanitainformazione.it
Utenti unici: 762
Rassegna del 09/09/2021
Notizia del: 08/09/2021
Foglio:2/2

l'immunità di gregge entro due mesi

Le minacce possibili

«I rischi sono sostanzialmente due – aggiunge il vicepresidente della FIASO – : i dati operativi, come quelli del sistema di prenotazione di visite specialistiche, dell'accettazione di un ricovero o di presa in carico al Pronto soccorso, possono essere criptati. Oppure questi stessi dati possono finire sul mercato nero. Quest'ultimo rischio, in un Paese come l'Italia dotato di un sistema sanitario pubblico, è meno cogente. **Più pericolosa, invece, la criptazione dei dati**. In una condizione di emergenza, le nostre aziende sono in grado di lavorare anche senza l'informatizzazione, ritornando ad utilizzare la "vecchia" carta. Un ospedale deve necessariamente accogliere e curare i pazienti. Ma questo meccanismo alternativo può reggere non oltre le 48 ore».

Come difendersi

L'unica soluzione possibile, dunque, pare essere impedire agli hacker di entrare nei nostri sistemi. Come? «Investendo una parte delle risorse del PNNR previste per lo sviluppo della digitalizzazione nella cybersecurity. **Lo smartworking e la telemedicina sono nuove porte d'accesso ai dati sanitari che, come tali, vanno adeguatamente tutelate**. Per garantire la sicurezza dei sistemi informativi sanitari è necessario che si investa in formazione di competenze specifiche e, più in generale, nella crescita di una cultura diffusa della prevenzione dei rischi informatici, in assenza della quale qualunque impegno di risorse potrebbe essere vanificato. Se finora le aziende produttrici dei dispositivi medici hanno certificato la qualità dei propri prodotti prima di immetterli sul mercato, da questo momento sarà necessario prevedere un'attestazione aggiuntiva che – conclude – ne attesti anche il grado di cybersecurity».

TAGS

cybersecurity Fiasо

ARTICOLI CORRELATI

Scuola, appello ai pediatri: «Parlate a genitori e ragazzi, il vaccino è fondamentale per la didattica in presenza»

Di Mauro (SIPPS) punta sulla corretta informazione scientifica per fugare dubbi e paure. Barbi (FIASO): «I giovani chiedono di vaccinarsi, mentre i genitori temono effetti collaterali a lunga scadenza. È importante tranquillizzarli»

di Federica Bosco

La "calda" estate di medici e professionisti sanitari.