Cronaca

Cybercrime: esperti, prossimo 11/9 sarà attacco informatico

'Non facciamoci trovare impreparati o conseguenze catastrofiche'



(ANSA) - ROMA, 03 MAR - Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio.

"Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo.

Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence".

Stamane si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (Cni). (ANSA).

AFFARI TECNICI

Stati Generali ingegneria dell'informazione

NOTIZIE DALLE PROFESSIONI

01/03/2022 di Redazione

Cyberguerra e crimini digitali: la pnademia e la guerra intensificheranno gli attacchi e le minacce cyber

Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Nessuno è al sicuro dai rischi cibernetici. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione "sicurezza informatica" al centro dei riflettori.

PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 saranno al centro di un dibattito che si terrà presso la Sala Capitolare del Senato della Repubblica giovedì 3 marzo alle ore 9,00 nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI).

Un evento al quale parteciperanno parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I) e Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS).

L'evento sarà trasmesso in diretta webTv del Senato della Repubblica: **webtv.senato.it**

LA SICILIA

Senato, crimini digitali, “Siamo tutti sotto attacco, serve piú consapevolezza”. Gli ingegneri: “Pronti a fare la nostra parte”

Di **Redazione** 03 mar 2022

Nel corso degli Stati Generali dell'Ingegneria dell'Informazione si è parlato di cyberguerra e di attacchi informatici sempre più diffusi

Milano, 3 marzo 2022. Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerrain corso tra Russia e Ucraina ha drammaticamente messo la questione “sicurezza informatica” sotto i riflettori.

UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERI

Si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneriadell'Informazione promossi dall'IntergruppoParlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri(CNI).

Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare InclusioneDigitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)

LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE»

«Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese».

I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente.

KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO»

«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre

necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity».

«L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO»

Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio.

«Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan UmitUygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence».

PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS

«La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha spiegato Luisa Franchina - Con la crisi Russia – Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».

DIGITALIZZAZIONE, GLI INGEGNERI: “PRONTI A FARE LA NOSTRA PARTE”

Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato ArmandoZambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I».

“Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali” ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I).

UFFICIO STAMPA

Barbara Carbone 335.441874

Aggiornato Venerdi' 04 marzo 2022 ore 14:35

Senato, Crimini Digitali

Siamo tutti sotto attacco, serve più consapevolezza. Cyberguerra e attacchi informatici sempre più diffusi. Gli Ingegneri: " Pronti a fare la nostra parte".

(AGR) Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione “sicurezza informatica” sotto i riflettori.

UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERI

Si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell’ambito degli Stati Generali dell’Ingegneria dell’Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI).
Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell’Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)

LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE»

«Gli Stati Generali Ingegneria dell’Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese».

I dati raccolti dall’azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente.

KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO»

«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. E’ inoltre necessario lavorare per risolvere il problema dell’assenza di

talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity».

«L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO»

Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio.

«Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence».

PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS

«La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha spiegato Luisa Franchina - Con la crisi Russia – Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».

DIGITALIZZAZIONE, GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE"

Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto, sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I».

"Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali" ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I).

Partecipa anche tu affinche' l'informazione vera e trasparente sia un bene per tutti

Adnkronos

Senato, crimini digitali, “Siamo tutti sotto attacco, serve più consapevolezza”. Gli ingegneri: “Pronti a fare la nostra parte”

03 marzo 2022 | 14.24

Nel corso degli Stati Generali dell’Ingegneria dell’Informazione si è parlato di cyberguerra e di attacchi informatici sempre più diffusi

Milano, 3 marzo 2022. Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la **guerra in corso tra Russia e Ucraina** ha drammaticamente messo la questione “**sicurezza informatica**” sotto i riflettori.

UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERI

Si è parlato di **PNRR**, **transizione digitale, cybersecurity, sanità digitale e industria 4.0** nel dibattito che si svolto questa mattina presso la **Sala Capitolare del Senato della Repubblica** nell’ambito degli **Stati Generali dell’Ingegneria dell’Informazione** promossi dall'**Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI)**.

Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice **Urania Papatheu**, **Presidente Intergruppo Parlamentare Inclusione Digitale**, **Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD**, Armando Zambrano, **Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino**, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell’Informazione (C3I), **Luisa Franchina**, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)

LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE»

«Gli Stati Generali Ingegneria dell’Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto **Urania Papatheu**- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese».

I dati raccolti dall’azienda globale per la cybersicurezza **Kaspersky** sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente.

KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO»

«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato **Cesare D'Angelo, General Manager Italy di Kaspersky** intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell’assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity».

«L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO»

Secondo il Global Risk Report per il 2021 del **World Economic Forum**, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio.

«Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto **Stefan UmitUygur**, **Ceo di 4Securitas**- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence».

PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS

«La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha spiegato **Luisa Franchina** - Con la crisi Russia – Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».

DIGITALIZZAZIONE, GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE"

Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato **Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI)** - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla **transizione digitale** prevista nell'ambito del **Pnrr** e al delicato tema della **cybersecurity**. Ma anche allo stretto rapporto tra **ingegneria e sanità digitale**, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I».

"Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali" ha dichiarato **Alessandro Astorino**, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I).

UFFICIO STAMPA

Barbara Carbone 335.441874

hellacarbone@hotmail.com

La voce d'Italia

Cybercrime: esperti, prossimo 11/9 sarà attacco informatico

Ultima Ora Marzo 3, 2022 ansa

(ANSA) – ROMA, 03 MAR – Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. "Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence". Stamane si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (Cni). Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del Mitd, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (Cni), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (Cestudis) (ANSA).



Kaspersky partecipa agli Stati Generali dell'Ingegneria dell'Informazione

Danilo Battista 1 giorno ago Hi Tech, Nerdangolo

SENATO, CRIMINI DIGITALI, "SIAMO TUTTI SOTTO ATTACCO,
SERVE PIÚ CONSAPEVOLEZZA". GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE"
NEL CORSO DEGLI STATI GENERALI DELL'INGEGNERIA DELL'INFORMAZIONE SI È PARLATO DI CYBERGUERRA E DI ATTACCHI INFORMATICI SEMPRE PIÙ DIFFUSI

Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione "sicurezza informatica" sotto i riflettori.

UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERI

Si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI).

Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)

LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE»

«Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese».
I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente.

KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO»

«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci – oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity».

«L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO»

Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio.
«Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence».

PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS

«La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche – ha spiegato Luisa Franchina – Con la crisi Russia – Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».

DIGITALIZZAZIONE, GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE"

Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) – I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I».
"Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle

infrastrutture digitali nazionali" ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I).

LIBERO QUOTIDIANO

Senato, crimini digitali, "Siamo tutti sotto attacco, serve piú consapevolezza". Gli ingegneri: "Pronti a fare la nostra parte"



03 marzo 2022

- Nel corso degli Stati Generali dell'Ingegneria dell'Informazione si è parlato di cyberguerra e di attacchi informatici sempre più diffusi

Milano, 3 marzo 2022. Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerrain corso tra Russia e Ucraina ha drammaticamente messo la questione "sicurezza informatica" sotto i riflettori.
UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERI
Si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneriadell'Informazione promossi dall'IntergruppoParlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri(CNI).
Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare InclusioneDigitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)
LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE»
«Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese».
I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente.
KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO»
«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di

Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity».
«L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO»
Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio.
«Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan UmitUygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence».
PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS
«La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha spiegato Luisa Franchina - Con la crisi Russia – Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».
DIGITALIZZAZIONE, GLI INGEGNERI: “PRONTI A FARE LA NOSTRA PARTE”
Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato ArmandoZambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I».
“Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali” ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I).
UFFICIO STAMPA
Barbara Carbone 335.441874
hellacarbone@hotmail.com

affaritaliani.it 26 ANNI ONLINE DAL 1996
Il primo quotidiano digitale, dal 1996

3 marzo 2022- 14:24

Senato, crimini digitali, “Siamo tutti sotto attacco, serve piú consapevolezza”. Gli ingegneri: “Pronti a fare la nostra parte”

(Adnkronos) - Nel corso degli Stati Generali dell’Ingegneria dell’Informazione si è parlato di cyberguerra e di attacchi informatici sempre più diffusiMilano, 3 marzo 2022. Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo

aumento dei crimini digitali, la guerrain corso tra Russia e Ucraina ha drammaticamente messo la questione “sicurezza informatica” sotto i riflettori. UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERISi è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell’ambito degli Stati Generali dell’Ingegneriadell’Informazione promossi dall'IntergruppoParlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri(CNI). Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare InclusioneDigitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell’Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE»«Gli Stati Generali Ingegneria dell’Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese».I dati raccolti dall’azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente. KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO»«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell’assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity». «L’ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO»Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan UmitUygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l’area interessata dal conflitto, provocando un’escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS«La pandemia ha proiettato il mondo in avanti di vent’anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha spiegato Luisa Franchina - Con la crisi Russia – Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».DIGITALIZZAZIONE, GLI INGEGNERI: “PRONTI A FARE LA NOSTRA PARTE”Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell’Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato ArmandoZambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell’informazione. Del resto sono diversi i settori nei quali il ruolo dell’ingegnere dell’informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell’ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l’attività del CNI negli ultimi tempi, soprattutto attraverso l’azione del Comitato C3I».“Gli ingegneri dell’informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali” ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l’ingegneria dell’informazione (C3I).UFFICIO STAMPA Barbara Carbone 335.441874hellacarbone@hotmail.com

IL GIORNALE D'ITALIA

Il Quotidiano Indipendente

"La libertà al singolare esiste solo nelle libertà al plurale"

Benedetto Croce

Senato, crimini digitali, "Siamo tutti sotto attacco, serve piú consapevolezza". Gli ingegneri: "Pronti a fare la nostra parte"

03 Marzo 2022

(Adnkronos) - Nel corso degli Stati Generali dell'Ingegneria dell'Informazione si è parlato di cyberguerra e di attacchi informatici sempre più diffusi

Milano, 3 marzo 2022. Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerrain corso tra Russia e Ucraina ha drammaticamente messo la questione "sicurezza informatica" sotto i riflettori.

UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERI

Si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneriadell'Informazione promossi dall'IntergruppoParlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri(CNI).

Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare InclusioneDigitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)

LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE»

«Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu-

Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese».

I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente.

KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO»

«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity».

«L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO»

Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio.

«Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan UmitUygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence».

PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS

«La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha spiegato Luisa Franchina - Con la crisi Russia – Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».

DIGITALIZZAZIONE, GLI INGEGNERI: “PRONTI A FARE LA NOSTRA PARTE”

Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell’Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato ArmandoZambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell’informazione. Del resto sono diversi i settori nei quali il ruolo dell’ingegnere dell’informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell’ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l’attività del CNI negli ultimi tempi, soprattutto attraverso l’azione del Comitato C3I».

“Gli ingegneri dell’informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali” ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l’ingegneria dell’informazione (C3I).

UFFICIO STAMPA

Barbara Carbone 335.441874

hellacarbone@hotmail.com

L’informazione indipendente
AgenParl

Digitale: domani in Senato Stati generali ingegneria dell’informazione

(AGENPARL) – mer 02 marzo 2022 Digitale: domani in Senato Stati generali ingegneria dell'informazione

Cyber attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Nessuno è al sicuro dai rischi cibernetici. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione "sicurezza informatica" al centro dei riflettori. Pnrr, transizione digitale, cybersecurity, sanità digitale e industria 4.0 saranno al centro di un dibattito che si terrà presso la sala Capitolare del Senato della Repubblica domani, giovedì 3 marzo, alle ore 9, nell'ambito degli Stati generali dell'ingegneria dell'informazione su iniziativa del presidente dell'intergruppo parlamentare inclusione digitale, senatrice Urania Giulia Papatheu, insieme ai colleghi parlamentari dell'Intergruppo ed in collaborazione con il Consiglio nazionale degli ingegneri (Cni). Aprirà i lavori la senatrice Urania Papatheu, presidente Intergruppo parlamentare inclusione digitale e parteciperanno tra i tanti ospiti Mauro Minenna, capo dipartimento per la Trasformazione digitale del Mitd, Armando Zambrano, presidente Consiglio nazionale Ingegneri (Cni), Alessandro Astorino, coordinatore Consiglio operativo Comitato italiano ingegneria dell'informazione (C3I) e Luisa Franchina, vicepresidente Centro studi Difesa e Sicurezza (CESTUDIS). L'evento sarà trasmesso in diretta webtv su webtv.senato.it.

Ufficio Stampa
Forza Italia-Berlusconi Presidente
Senato della Repubblica

SENATO : CRIMINI DIGITALE " SIAMO TUTTI SOTTO ATTACCHI "

3 Marzo 2022/0 Commenti/in ATTUALITA', NEWS /da Alberto Alovisi

SENATO, CRIMINI DIGITALI,
"SIAMO TUTTI SOTTO ATTACCO,
SERVE PIÚ CONSAPEVOLEZZA".
GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE"

NEL CORSO DEGLI STATI GENERALI DELL'INGEGNERIA DELL'INFORMAZIONE SI È PARLATO DI CYBERGUERRA E DI ATTACCHI INFORMATICI SEMPRE PIÙ DIFFUSI

Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la **guerra in corso tra Russia e Ucraina** ha drammaticamente messo la questione "**sicurezza informatica**" sotto i riflettori.

UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERI

Si è parlato di **PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0** nel dibattito che si svolto questa mattina presso la **Sala Capitolare del Senato della Repubblica** nell'ambito degli **Stati Generali dell'Ingegneria dell'Informazione** promossi dall'**Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI).**

Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice **Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD**, Armando Zambrano, **Presidente Consiglio Nazionale Ingegneri (CNI)**, **Alessandro Astorino**, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), **Luisa Franchina**, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)

LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE»

«Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto **Urania Papatheu**– Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese».

I dati raccolti dall'azienda globale per la cybersicurezza **Kaspersky** sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente.

KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO»

«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato **Cesare D'Angelo, General Manager Italy di Kaspersky i**ntervistato dal caporedattore di Economy Francesco Condoluci – oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. E' inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity».

«L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO»

Secondo il Global Risk Report per il 2021 del **World Economic Forum**, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto **Stefan Umit Uygur, Ceo di 4Securitas**– Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence».

PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS

«La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche – ha spiegato **Luisa Franchina** – Con la crisi Russia – Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».

DIGITALIZZAZIONE, GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE"

Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato **Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) –** I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco

alla **transizione digitale** prevista nell'ambito del **Pnrr** e al delicato tema della **cybersecurity**. Ma anche allo stretto rapporto tra **ingegneria e sanità digitale**, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I».
"Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali" ha dichiarato **Alessandro Astorino**, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I).

UFFICIO STAMPA

Barbara Carbone 335.441874

hellacarbone@hotmail.com

Carola Assumma Comunicazione

carola.assumma@carolaassummacomunicazione.com

venerdì, Marzo 4, 2022

dietrolanotizia.it
www.dietrolanotizia.eu
Quotidiano on-line

ATTUALITA'

Cyberguerra: attacchi informatici sempre più diffusi



Senato, crimini digitali, “siamo tutti sotto attacco, serve piú consapevolezza”. Gli ingegneri: “pronti a fare la nostra parte”

Nel corso degli stati generali dell’ingegneria dell’informazione si è parlato di cyberguerra e di attacchi informatici sempre più diffusi

Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione “sicurezza informatica” sotto i riflettori.

UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERI

Si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell’ambito degli Stati Generali dell’Ingegneria dell’Informazione promossi dall’Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI).

Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell’Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)

LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE»

«Gli Stati Generali Ingegneria dell’Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese». I dati raccolti dall’azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all’anno precedente.

KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO»

«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all’adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D’Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci – oggi è estremamente importante migliorare l’alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica.

E’ inoltre necessario lavorare per risolvere il problema dell’assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity».

«L’ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO»

Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence».

PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS

«La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche – ha spiegato Luisa Franchina – Con la crisi Russia – Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».

DIGITALIZZAZIONE, GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE"

Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) – I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione.

Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I».

"Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali" ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I).

IMMEDIAPRESS/SENATO, CRIMINI DIGITALI, "SIAMO TUTTI SOTTO ATTACCO, SERVE PIU' CONSAPEVOLEZZA". GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE"

3 Marzo 2022

ADN0853 7 ECO 0 ADN ECO NAZ IMMEDIAPRESS/SENATO, CRIMINI DIGITALI, "SIAMO TUTTI SOTTO ATTACCO, SERVE PIU' CONSAPEVOLEZZA". GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE" = (Adnkronos) –
Nel corso degli Stati Generali dell'Ingegneria dell'Informazione si è parlato di cyberguerra e di attacchi informatici sempre più diffusi Milano, 3 marzo 2022. Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si

era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione "sicurezza informatica" sotto i riflettori.
UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERI
Si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri(CNI). Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS) LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE» «Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese». I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente. KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO» «Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco CONDOLUCI - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity». «L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO» Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan UmitUygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS «La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha spiegato Luisa Franchina - Con la crisi Russia - Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe». DIGITALIZZAZIONE, GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE" Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei

confronti di questi temi - ha sottolineato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I». "Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali" ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I). Immediapress è un servizio di diffusione di comunicati stampa in testo originale redatto direttamente dall'ente che lo emette. L'Adnkronos e Immediapress non sono responsabili per i contenuti dei comunicati trasmessi (Imm- Kaspersky) ISSN 2465 - 1222 03-MAR-22 14:25

TE news.

Cybercrime: esperti, prossimo 11/9 sarà attacco informatico

ANSA

Di **Ansa**

03/03/2022

(ANSA) – ROMA, 03 MAR – Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. "Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe

coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence". Stamane si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (Cni). (ANSA).

DIR2156 3 CRO 0 RR1 N/POL / DIR /TXT DIGITALE. INGEGNERI IN SENATO SU CYBERSICUREZZA: PRONTI A FARE NOSTRA PARTE -2- (DIRE)

Roma, 3 mar. - Inoltre: KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO» - «Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco CONDOLUCI - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. E' inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity». «L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO» - Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». (SEGUE) (Red/ Dire) 15:22 03-03-22 NNNN

IL MESSAGGERO

Sicurezza informatica, gli esperti al Senato: «Il prossimo 11 settembre potrebbe essere un attacco cyber»

Si sono svolti oggi al Senato gli Stati Generali Ingegneria dell'Informazione



Giovedì 3 Marzo 2022, 15:06

Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione "sicurezza informatica" sotto i riflettori.

Tavola rotonda al Senato su transizione digitale e cybersecurity

Si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto il 3 marzo presso la Sala Capitolare del Senato della Repubblica nell'ambito degli **Stati Generali dell'Ingegneria dell'Informazione** promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI).

Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)

CPR:
Il distretto Marche in cerca di rilancio punta sul robot per fare le scarpe

«La minaccia informatica è allarmante»

«Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese». I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente.

Kaspersky: «individuati 20mila file malevoli in più al giorno»

«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante **migliorare l'alfabetizzazione digitale** e aumentare la consapevolezza in materia di sicurezza informatica. E' inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity».

Ucraina, Anonymous dichiara cyberguerra alla Russia: hackerate banche, televisioni e ferrovie. "Anche l'Italia tra gli obiettivi"

Anonymous, attacco hacker ai siti governativi russi. Facebook e Twitter rispondono al blocco di Mosca

L'esalation Cyber potrebbe coinvolgere tutto il mondo

Secondo il **Global Risk Report** per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio.

«Personalmente credo che il prossimo potenziale '**11 settembre' sarà rappresentato da un attacco informatico** che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto **Stefan Umit Uygur**, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence».

«La **pandemia** ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha spiegato Luisa Franchina - Con la crisi Russia – **Ucraina** gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».

Ucraina sotto attacco, Anonymous alza il tiro: sotto attacco Gazprom e le grandi finanziarie

Ucraina, Anonymous dichiara cyberguerra alla Russia: «In ostaggio i vostri sistemi di controllo»

Digitalizzazine, gli ingegneri: «pronti a fare la nostra parte»

Per promuovere la diffusione della **cultura digitale** e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I».

"Gli **ingegneri dell'informazione** sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali" ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I).

Avvenire

Il Cestudis: col conflitto crescono i crimini digitali

Se già con la pandemia si era registrato un forte aumento dei crimini digitali, la guerra tra Russia e Ucraina ha drammaticamente messo la questione della sicurezza informatica sotto i riflettori. «La pandemia ha proiettato il mondo in avanti di 20 anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche», ha spiegato Luisa Franchina, vice presidente del Centro studi difesa e sicurezza. «Con la crisi Russia-Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe», prosegue Franchina. Del tema si è discusso nel corso del dibattito che si svolto ieri mattina presso la Sala capitolare del Senato nell'ambito degli Stati Generali promossi dall'Intergruppo parlamentare Inclusione digitale e dal Cni-Consiglio nazionale degli ingegneri. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha evidenziato Armando Zambrano, presidente del Cni –. I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del Cni negli ultimi tempi».

Economy Magazine

4 marzo 2022

Crimini digitali, allarme dal Senato: siamo tutti sotto attacco

Di cyberguerra e degli attacchi informatici sempre più diffusi si è parlato nel corso degli Stati generali dell'Ingegneria dell'Informazione tenutisi nella Sala Capitolare di Piazza della Minerva alla presenza di esperti di cybersicurezza, analisti e parlamentari

Redazione Web
-
04/03/2022



Da sinistra: Stefan Uygur, Alberto Pagani, Francesco Condoluci e Cesare D'Angelo

Se già con la pandemia si era registrato un **aumento esponenziale dei crimini digitali** (il cui impatto economico globale si avvicina secondo le stime al **6% del Pil mondiale**), la **guerra in corso tra Russia e Ucraina** ha drammaticamente messo la questione **"sicurezza informatica"**sotto i riflettori di tutta la comunità internazionale.

Una tavola rotonda promossa dal Consiglio Nazionale degli Ingegneri

Siamo praticamente a un passo da «un **nuovo 11 settembre informatico**». Così **Stefan Umit Uygur,** esperto di cybersecurity e Ceo della startup 4Securitas ha riassunto il livello di rischio che pende come una spada di Damocle sulle nostre economie, sulla società e sulla stessa tenuta delle **democrazie, sempre più dipendenti dall'ecosistema digitale**. L'allarme è risuonato nel contesto istituzionale della **Sala Capitolare del Senato della Repubblica** dove a discutere di cyber attacks e della loro minaccia crescente (ma anche di PNRR e digital transformation, sanità digitale e industria 4.0) si sono ritrovati parlamentari analisti ed esperti di transizione digitale nell'ambito di una **tavola rotonda** promossa dall'**Intergruppo Parlamentare Inclusione Digitale** e dal **Consiglio Nazionale degli Ingegneri (CNI).** Nel corso del dibattito Uygur, intervistato dal caporedattore di **Economy** e responsabile online, Francesco Condoluci, ha ipotizzato appunto che se ci dovesse essere «un nuovo 11 settembre», la forma sarà quella di «un **attacco informatico globale**, mirato a colpire tutto il sistema digitale». «Per difendersi e crescere solidamente – ha aggiunto – **serve una cultura digitale** che abbia una prospettiva globale. Serve una promozione degli **studi accademici nel settore**. «La forte accelerazione nel mondo digitale dovuta alla pandemia – gli ha fatto eco **Luisa Franchina**, **vicepresidente del Centro Studi Difesa e Sicurezza** ha portato ad un'impennata degli attacchi, soprattutto verso aziende sanitarie e farmaceutiche. La prova che si tratti di una vera e propria guerra diffusa la si ha guardando al **conflitto Russia-Ucraina**, dove gli attacchi cyber sono iniziati prima di quelli cinetici» ha .

La senatrice Urania Papatheu (FI): «Minaccia informatica è allarmante»

«Gli Stati Generali dell'ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale – ha commentato nel suo intervento **Urania Papatheu** – occorre dunque contrastare con determinazione un **fenomeno che mette a rischio la tenuta del Paese**». Il deputato **Alberto Pagani, componente della Commissione Difesa della Camera** ha fatto il punto su quanto l'Italia sta facendo per difendere le infrastrutture critiche: «Abbiamo da poco istituito l'**Agenzia Nazionale per la Cybersecurity**che ora va resa operativa, ma bisogna lavorare soprattutto sulla diffusione della **consapevolezza dei rischi**». Secondo il Global Risk Report per il 2021 del World Economic Forum, la **sicurezza**

informatica rappresenta infatti **una delle maggiori minacce** che l'umanità dovrà affrontare **nel prossimo decennio**.

Kaspersky: «Investiamo nella formazione dei giovani sulla cybersecurity»

«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce – ha spiegato **Cesare D'Angelo, General Manager di Kaspersky Italia** – oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. E' inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity».

Digitalizzazione, «gli ingegneri faranno la loro parte»

Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato A**rmando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI)** – I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I». «Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali» ha dichiarato **Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I).**

UCRAINA: GUERRA E CYBERSECURITY, ANCHE LE AZIENDE SI DEVONO DIFENDERE
Body
UCRAINA: GUERRA E CYBERSECURITY, ANCHE LE AZIENDE SI DEVONO DIFENDERE = Sono 4 le azioni necessarie in questo periodo contro il cybercrime e per contrastare due nuovi malware: HermeticWiper e Cyclops Blink Varese, 3 mar. (Adnkronos/Labitalia) - In questo periodo di forti tensioni internazionali e di vera e propria guerra sul fronte ucraino, anche le aziende devono alzare la difesa contro i gruppi di cybercriminali. Questi gruppi stanno sfruttando il momento di crisi per attaccare indistintamente e violentemente le aziende di qualsiasi dimensione. Diventa sempre più necessario quindi mettere in campo politiche di difesa, specialmente nel caso in cui un'azienda abbia filiali e relazioni dirette con la Russia e l'Ucraina. CybergON, business unit di Elmec Informatica dedicata alla sicurezza informatica, ha stilato le 4 principali azioni di mitigazione che le aziende

devono mettere in atto. Eccole: 1) Innalzare il livello di priorità nel monitoraggio di eventi che coinvolgano sistemi presenti in Ucraina e/o Russia. 2) Prestare attenzione a eventi che coinvolgono IP pubblici indicati nelle [liste del Cert](https://csirt.gov.it/contenuti/ucraina-pubblicati-nuovi-importanti-ed-urgenti-ioc-al01-220224-csirt-ita) e in generale da IP pubblici assegnati a Russia o Ucraina. 3) Monitorare tutti gli accessi a piattaforme sensibili, come Office 365 e Azure, che provengono dai paesi a rischio. 4) Mantenere aggiornati gli Indicator Of Compromise (Ioc) identificati a livello internazionale e consigliati dal Cert Europeo sugli strumenti di detection. Infine, è importante adottare pratiche di patching dei tool con vulnerabilità note e innalzare il livello di consapevolezza interno dei rischi legati; ad esempio, le email di phishing, contribuiranno a diminuire il rischio e la superficie di attacco. (segue) (Map/Adnkronos) ISSN 2465 - 1222 03-MAR-22 15:53 NNNN

UCRAINA: ESPERTI, CON COVID E GUERRA AUMENTO CRIMINI DIGITALI

Body

CRO S0A QBXB UCRAINA: ESPERTI, CON COVID E GUERRA AUMENTO CRIMINI DIGITALI (v. «Cybercrime..» delle ore 12:09) (ANSA) - ROMA, 03 MAR - Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione «sicurezza informatica» sotto i riflettori. «La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche», ha spiegato Luisa Franchina Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS). «Con la crisi Russia - Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe», proegue Franchina. Del tema si è discusso nel corso del dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI). Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese - è stato sottolineato - è fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi - ha evidenziato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I». «Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali» ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I). (ANSA). VR 03-MAR-22 12:34 NNNN

UCRAINA:ESPERTI, CON COVID E GUERRA AUMENTO CRIMINI DIGITALI

Body

CRO S0B QBXB UCRAINA:ESPERTI, CON COVID E GUERRA AUMENTO CRIMINI DIGITALI (v. «Cybercrime..» delle ore 12:09) (ANSA) - ROMA, 03 MAR - Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione «sicurezza informatica» sotto i riflettori. «La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche», ha spiegato Luisa Franchina Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS). «Con la crisi Russia - Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe», proegue Franchina. Del tema si è discusso nel corso del dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali

dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI). Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese - è stato sottolineato - è fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi - ha evidenziato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I». «Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali» ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I). (ANSA). VR 03-MAR-22 12:34 NNNN

YBERCRIME: ESPERTI, 20 MILA FILE MALEVOLI IN PIÙ AL GIORNO
Body
CRO S0A QBXB CYBERCRIME: ESPERTI, 20 MILA FILE MALEVOLI IN PIÙ AL GIORNO Nel 2021 rispetto al 2020 anche per aumento attività on line (ANSA) - ROMA, 03 MAR - I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente. «Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce - ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity». Del tema si è discusso nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI). «Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese»¯. (ANSA). VR 03-MAR-22 12:19 NNNN
CYBERCRIME: ESPERTI, 20 MILA FILE MALEVOLI IN PIÙ AL GIORNO

CRO S0B QBXB CYBERCRIME: ESPERTI, 20 MILA FILE MALEVOLI IN PIÙ AL GIORNO Nel 2021 rispetto al 2020 anche per aumento attività on line (ANSA) - ROMA, 03 MAR - I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente. «Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce - ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity». Del tema si è discusso nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI). «Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica

è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese»¯. (ANSA). VR 03-MAR-22 12:19 NNNN

CYBERCRIME: ESPERTI, PROSSIMO 11/9 SARÀ ATTACCO INFORMATICO
Body
CRO S0B QBXB CYBERCRIME: ESPERTI, PROSSIMO 11/9 SARÀ ATTACCO INFORMATICO 'Non facciamoci trovare impreparati o conseguenze catastrofichè (ANSA) - ROMA, 03 MAR - Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembrè sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». Stamane si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (Cni). Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del Mitd, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (Cni), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (Cestudis) (ANSA). VR 03-MAR-22 12:09 NNNN

CYBERCRIME: ESPERTI, PROSSIMO 11/9 SARÀ ATTACCO INFORMATICO
Body
CRO S0A QBXB CYBERCRIME: ESPERTI, PROSSIMO 11/9 SARÀ ATTACCO INFORMATICO 'Non facciamoci trovare impreparati o conseguenze catastrofichè (ANSA) - ROMA, 03 MAR - Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembrè sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». Stamane si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (Cni). Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del Mitd, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri

(Cni), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (Cestudis) (ANSA). VR 03-MAR-22 12:09 NNNN

MMEDIAPRESS/SENATO, CRIMINI DIGITALI, «SIAMO TUTTI SOTTO ATTACCO, SERVE PIÙ CONSAPEVOLEZZA». GLI INGEGNERI: «PRONTI A FARE LA NOSTRA PARTE» = (Adnkronos) - Nel corso degli Stati Generali dell'Ingegneria dell'Informazione si è parlato di cyberguerra e di attacchi informatici sempre più diffusi Milano, 3 marzo 2022. Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione «sicurezza informatica» sotto i riflettori. UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERI Si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri(CNI). Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS) LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE» «Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese». I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente. KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO» «Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity». «L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO» Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembrè sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan UmitUygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS «La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha spiegato Luisa Franchina - Con la crisi Russia - Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe». DIGITALIZZAZIONE, GLI INGEGNERI:

«PRONTI A FARE LA NOSTRA PARTE» Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi - ha sottolineato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I». «Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali» ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I). Immediapress è un servizio di diffusione di comunicati stampa in testo originale redatto direttamente dall'ente che lo emette. L'Adnkronos e Immediapress non sono responsabili per i contenuti dei comunicati trasmessi (Imm- Kaspersky) ISSN 2465 - 1222 03-MAR-22 14:25 NNNN

CYBERSECURITY: STATI GENERALI INGEGNERIA INFORMAZIONE, A RISCHIO TENUTA PAESE

Body

CYBERSECURITY: STATI GENERALI INGEGNERIA INFORMAZIONE, A RISCHIO TENUTA PAESE = Roma, 3 mar. (Adnkronos/Labitalia) - Si è parlato di Pnrr, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto oggi nell'ambito degli Stati generali dell'ingegneria dell'informazione promossi dall'Intergruppo parlamentare inclusione digitale e dal Consiglio nazionale degli ingegneri (Cni). Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, presidente Intergruppo parlamentare inclusione digitale, Mauro Minenna, capo dipartimento per la trasformazione digitale del Mitd, Armando Zambrano, presidente Consiglio nazionale ingegneri (Cni), Alessandro Astorino, coordinatore consiglio operativo comitato italiano ingegneria dell'informazione (C3I), Luisa Franchina, vice presidente Centro studi difesa e sicurezza (Cestudis) «Gli Stati generali ingegneria dell'informazione - ha detto Urania Papatheu- rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale. Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese». I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente. «Si tratta - ha spiegato Cesare D'Angelo, general manager Italy di Kaspersky - di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce. Oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity». (segue) (Dks/Adnkronos) ISSN 2465 - 1222 03-MAR-22 13:36 NNNN

CYBERSECURITY: STATI GENERALI INGEGNERIA INFORMAZIONE, A RISCHIO TENUTA PAESE (2)

Body

CYBERSECURITY: STATI GENERALI INGEGNERIA INFORMAZIONE, A RISCHIO TENUTA PAESE (2) = (Adnkronos/Labitalia) - «Personalmente - ha detto Stefan Umit Uygur, ceo di 4Securitas - credo che il prossimo potenziale '11 settembrè sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema Non possiamo farci trovare

impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». «La pandemia - ha spiegato Luisa Franchina - ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche. Con la crisi Russia-Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe». Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo - ha sottolineato Armando Zambrano presidente del Cni -registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del Cni negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I». «Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali» ha dichiarato Alessandro Astorino, coordinatore del consiglio operativo del comitato italiano per l'ingegneria dell'informazione (C3I). (Dks/Adnkronos) ISSN 2465 - 1222 03-MAR-22 13:36 NNNN

UCRAINA:ESPERTI, CON COVID E GUERRA AUMENTO CRIMINI DIGITALI
Body
CRO S0A QBXB UCRAINA:ESPERTI, CON COVID E GUERRA AUMENTO CRIMINI DIGITALI (v. «Cybercrime..» delle ore 12:09) (ANSA) - ROMA, 03 MAR - Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione «sicurezza informatica» sotto i riflettori. «La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche», ha spiegato Luisa Franchina Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS). «Con la crisi Russia - Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe», proegue Franchina. Del tema si è discusso nel corso del dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI). Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese - è stato sottolineato - è fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi - ha evidenziato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I». «Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali» ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I). (ANSA). VR 03-MAR-22 12:34 NNNN

UCRAINA:ESPERTI, CON COVID E GUERRA AUMENTO CRIMINI DIGITALI
Body

CRO S0B QBXB UCRAINA:ESPERTI, CON COVID E GUERRA AUMENTO CRIMINI DIGITALI (v. «Cybercrime..» delle ore 12:09) (ANSA) - ROMA, 03 MAR - Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione «sicurezza informatica» sotto i riflettori. «La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche», ha spiegato Luisa Franchina Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS). «Con la crisi Russia - Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe», proegue Franchina. Del tema si è discusso nel corso del dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI). Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese - è stato sottolineato - è fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi - ha evidenziato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I». «Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali» ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I). (ANSA). VR 03-MAR-22 12:34 NNNN

CYBERCRIME: ESPERTI, PROSSIMO 11/9 SARÀ ATTACCO INFORMATICO

Body

CRO S0B QBXB CYBERCRIME: ESPERTI, PROSSIMO 11/9 SARÀ ATTACCO INFORMATICO 'Non facciamoci trovare impreparati o conseguenze catastrofichè (ANSA) - ROMA, 03 MAR - Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembrè sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». Stamane si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (Cni). Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del Mitd, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (Cni), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (Cestudis) (ANSA). VR 03-MAR-22 12:09 NNNN

CYBERCRIME: ESPERTI, PROSSIMO 11/9 SARÀ ATTACCO INFORMATICO

Body

CRO S0A QBXB CYBERCRIME: ESPERTI, PROSSIMO 11/9 SARÀ ATTACCO INFORMATICO 'Non facciamoci trovare impreparati o conseguenze catastrofichè (ANSA) - ROMA, 03 MAR - Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembrè sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». Stamane si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (Cni). Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del Mitd, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (Cni), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (Cestudis) (ANSA). VR 03-MAR-22 12:09 NNNN

UCRAINA: SICUREZZA DIGITALE, GIOVEDÌ CONVEGNO IN SENATO

Body

CRO S0B QBXB UCRAINA: SICUREZZA DIGITALE, GIOVEDÌ CONVEGNO IN SENATO (ANSA) - ROMA, 28 FEB - Pnrr, transizione digitale, cybersecurity, sanità digitale e industria 4.0 saranno al centro di un dibattito che si terrà nella Sala Capitolare del Senato della Repubblica giovedì 3 marzo alle 9 nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI)«. È quanto si legge in una nota. »Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati - è spiegato nella presentazione dell'evento - Nessuno è al sicuro dai rischi cibernetici. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione 'sicurezza informaticà al centro dei riflettori«. All'evento parteciperanno parlamentari, analisti ed esperti di transizione digitale. Tra questi la senatrice Urania Papatheu (Presidente Intergruppo Parlamentare Inclusione Digitale), Mauro Minenna (Capo Dipartimento per la Trasformazione Digitale del MITD), Armando Zambrano (presidente Consiglio Nazionale Ingegneri), Alessandro Astorino (coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione) e Luisa Franchina, vicepresidente Centro Studi Difesa e Sicurezza. L'evento sarà trasmesso in diretta webTv del Senato della Repubblica. (ANSA). TZ 28-FEB-22 17:05 NNNN

TRANSIZIONE DIGITALE: L'ORDINE DEGLI INGEGNERI DI FIRENZE, 'ACCELERARE NELLA PÀ (2)

Body

TRANSIZIONE DIGITALE: L'ORDINE DEGLI INGEGNERI DI FIRENZE, 'ACCELERARE NELLA PÀ (2) = (Adnkronos) - «La transizione digitale nella pubblica amministrazione - ha dichiarato Francesca Satta - è un aspetto centrale, nell'ottica di una maggiore semplificazione e di

servizi più immediati ed efficaci per i cittadini. Grazie al digitale possiamo migliorare l'organizzazione della Pubblica amministrazione ma la progettazione di sistemi ed infrastrutture richiede competenze e professionisti del settore. Non possiamo rischiare che questa sfida sia affidata ad improvvisazioni. Affidarsi ad ingegneri iscritti all'ordine significa scegliere professionisti con obbligo di formazione continua, con un codice deontologico da rispettare e con una assicurazione obbligatoria che tutela professionista e committenza». In totale sono sei i panel previsti: dopo i saluti istituzionali (ore 9.30) del presidente Intergruppo parlamentare inclusione digitale Urania Papatheu, del capo dipartimento per la trasformazione digitale del Ministero per l'innovazione tecnologica e la transizione digitale Mauro Minenna, del presidente del Consiglio nazionale ingegneri Armando Zambrano e del coordinatore del Consiglio operativo del comitato italiano ingegneria dell'informazione del Cni Alessandro Astorino, si parlerà di «Pnrr e transizione digitale» (ore 10), «Cyber attacks, minaccia crescente: la necessità di una consapevolezza diffusa» (ore 11), «Sanità digitale» (ore 12.20), «Industria 4.0» (ore 15.30), «Transizione digitale nella pubblica amministrazione» (ore 16.30) e si darà spazio ad alcuni casi di eccellenza di innovazione digitale (ore 17.30). (Zto/Adnkronos) ISSN 2465 - 1222 28-FEB-22 12:04 NNNN

MMEDIAPRESS/SENATO, CRIMINI DIGITALI, «SIAMO TUTTI SOTTO ATTACCO, SERVE PIÙ CONSAPEVOLEZZA». GLI INGEGNERI: «PRONTI A FARE LA NOSTRA PARTE» = (Adnkronos) - Nel corso degli Stati Generali dell'Ingegneria dell'Informazione si è parlato di cyberguerra e di attacchi informatici sempre più diffusi Milano, 3 marzo 2022. Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione «sicurezza informatica» sotto i riflettori. UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERI Si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri(CNI). Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS) LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE» «Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese». I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente. KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO» «Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity». «L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO» Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11

settembrè sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan UmitUygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS «La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha spiegato Luisa Franchina - Con la crisi Russia - Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe». DIGITALIZZAZIONE, GLI INGEGNERI: «PRONTI A FARE LA NOSTRA PARTE» Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi - ha sottolineato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I». «Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali» ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I). Immediapress è un servizio di diffusione di comunicati stampa in testo originale redatto direttamente dall'ente che lo emette. L'Adnkronos e Immediapress non sono responsabili per i contenuti dei comunicati trasmessi (Imm- Kaspersky) ISSN 2465 - 1222 03-MAR-22 14:25 NNNN

DIR2156 3 CRO 0 RR1 N/POL / DIR /TXT DIGITALE. INGEGNERI IN SENATO SU CYBERSICUREZZA: PRONTI A FARE NOSTRA PARTE -2- (DIRE) Roma, 3 mar. - Inoltre: KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO» - «Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco CONDOLUCI - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. E' inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity». «L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO» - Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove

competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». (SEGUE) (Red/ Dire) 15:22 03-03-22 NNNN

DIR2156 3 CRO 0 RR1 N/POL / DIR /TXT DIGITALE. INGEGNERI IN SENATO SU CYBERSICUREZZA: PRONTI A FARE NOSTRA PARTE -2- (DIRE) Roma, 3 mar. - Inoltre: KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO» - «Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco CONDOLUCI - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. E' inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity». «L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO» - Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». (SEGUE) (Red/ Dire) 15:22 03-03-22 NNNN

(ANSA) - ROMA, 03 MAR - Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio.

"Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo.

Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence".

Stamane si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneria dell'Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (Cni). (ANSA).

(AGR) Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione “sicurezza informatica” sotto i riflettori.

Si è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell’ambito degli Stati Generali dell’Ingegneria dell’Informazione promossi dall'Intergruppo Parlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri (CNI).
Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare Inclusione Digitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell’Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)

LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE»

«Gli Stati Generali Ingegneria dell’Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese».

I dati raccolti dall’azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente.

KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO»

«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. E’ inoltre necessario lavorare per risolvere il problema dell’assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity».

«L’ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO»

Secondo il Global Risk Report per il 2021 del World Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio.

«Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan Umit Uygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l’area interessata dal conflitto, provocando un’escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence».

PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS

«La pandemia ha proiettato il mondo in avanti di vent’anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha

spiegato Luisa Franchina - Con la crisi Russia – Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».

DIGITALIZZAZIONE, GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE"

Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato Armando Zambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I».

"Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali" ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I).

(Adnkronos) - Nel corso degli Stati Generali dell'Ingegneria dell'Informazione si è parlato di cyberguerra e di attacchi informatici sempre più diffusiMilano, 3 marzo 2022. Cyber Attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerrain corso tra Russia e Ucraina ha drammaticamente messo la questione "sicurezza informatica" sotto i riflettori. UNA TAVOLA ROTONDA VOLUTA DAL CONSIGLIO NAZIONALE INGEGNERISi è parlato di PNRR, transizione digitale, cybersecurity, sanità digitale e industria 4.0 nel dibattito che si svolto questa mattina presso la Sala Capitolare del Senato della Repubblica nell'ambito degli Stati Generali dell'Ingegneriadell'Informazione promossi dall'IntergruppoParlamentare Inclusione Digitale e dal Consiglio Nazionale degli Ingegneri(CNI). Un evento al quale hanno partecipato parlamentari, analisti e i massimi esperti di transizione digitale. Tra questi la senatrice Urania Papatheu, Presidente Intergruppo Parlamentare InclusioneDigitale, Mauro Minenna, Capo Dipartimento per la Trasformazione Digitale del MITD, Armando Zambrano, Presidente Consiglio Nazionale Ingegneri (CNI), Alessandro Astorino, Coordinatore Consiglio Operativo Comitato Italiano Ingegneria dell'Informazione (C3I), Luisa Franchina, Vice Presidente Centro Studi Difesa e Sicurezza (CESTUDIS)LA SENATRICE PAPATHEU (FI): «MINACCIA INFORMATICA È ALLARMANTE»«Gli Stati Generali Ingegneria dell'Informazione rappresentano un importante momento di confronto perché la minaccia informatica è sempre più attuale- ha detto Urania Papatheu- Occorre dunque contrastare con determinazione un fenomeno che mette a rischio la tenuta del Paese».I dati raccolti dall'azienda globale per la cybersicurezza Kaspersky sono allarmanti: nel 2021 sono stati individuati 20.000 file malevoli in più al giorno rispetto all'anno precedente. KASPERSKY: «INDIVIDUATI 20 MILA FILE MALEVOLI IN PIÚ AL GIORNO»«Si tratta di uno scenario piuttosto prevedibile poiché, in seguito all'adozione del lavoro da remoto in tutto il mondo, le attività svolte online si sono moltiplicate. Il numero di dispositivi utilizzati è aumentato a livello mondiale, comportando un ampliamento della superficie di attacco esposta alle minacce- ha spiegato Cesare D'Angelo, General Manager Italy di Kaspersky intervistato dal caporedattore di Economy Francesco Condoluci - oggi è estremamente importante migliorare l'alfabetizzazione digitale e aumentare la consapevolezza in materia di sicurezza informatica. È inoltre necessario lavorare per risolvere il problema dell'assenza di talenti. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity». «L'ESCALATION CYBER POTREBBE COINVOLGERE TUTTO IL MONDO»Secondo il Global Risk Report per il 2021 del World

Economic Forum, la sicurezza informatica rappresenta una delle maggiori minacce che l'umanità dovrà affrontare nel prossimo decennio. «Personalmente credo che il prossimo potenziale '11 settembre' sarà rappresentato da un attacco informatico che avrebbe però un impatto molto più grave, perché in questo caso diventerebbe un attacco globale non mirato a una singola nazione, ma all'intero sistema- ha detto Stefan UmitUygur, Ceo di 4Securitas- Non possiamo farci trovare impreparati, altrimenti le conseguenze saranno catastrofiche, come sta già avvenendo nella situazione Russia-Ucraina, in cui gli attacchi si propagano oltre l'area interessata dal conflitto, provocando un'escalation cyber che potrebbe coinvolgere tutto il mondo. Occorre dunque alzare il livello di consapevolezza diffusa e promuovere la formazione sulla sicurezza informatica, creando nuove competenze specifiche e adeguando la trasformazione digitale delle aziende e del Paese in ottica di cyber defence». PANDEMIA E GUERRA PREOCCUPANO GLI ESPERTI DEL CESTUDIS«La pandemia ha proiettato il mondo in avanti di vent'anni nella digitalizzazione e gli attacchi cibernetici mostrano una impennata soprattutto verso le aziende sanitarie e farmaceutiche - ha spiegato Luisa Franchina - Con la crisi Russia – Ucraina gli attacchi cyber sono iniziati, prima ancora di quelli cinetici e hanno coinvolto aziende pubbliche e private ucraine e russe».DIGITALIZZAZIONE, GLI INGEGNERI: "PRONTI A FARE LA NOSTRA PARTE"Per promuovere la diffusione della cultura digitale e del processo di digitalizzazione del Paese fondamentale è il ruolo degli ingegneri dell'Informazione. «Ormai da tempo registriamo un crescente interesse da parte dei giovani studenti nei confronti di questi temi – ha sottolineato ArmandoZambrano Presidente Consiglio Nazionale Ingegneri (CNI) - I nostri rapporti testimoniano come siano in costante aumento gli iscritti e i laureati in ingegneria dell'informazione. Del resto sono diversi i settori nei quali il ruolo dell'ingegnere dell'informazione potrà risultare determinante. Mi riferisco alla transizione digitale prevista nell'ambito del Pnrr e al delicato tema della cybersecurity. Ma anche allo stretto rapporto tra ingegneria e sanità digitale, a proposito del quale intensa è stata l'attività del CNI negli ultimi tempi, soprattutto attraverso l'azione del Comitato C3I»."Gli ingegneri dell'informazione sono al servizio del Paese per garantire la massima difesa cibernetica delle infrastrutture digitali nazionali" ha dichiarato Alessandro Astorino, coordinatore del Consiglio Operativo del Comitato italiano per l'ingegneria dell'informazione (C3I).

(AGENPARL) – mer 02 marzo 2022 Digitale: domani in Senato Stati generali ingegneria dell'informazione

Cyber attacks, una minaccia costante e che riguarda tutti, soggetti pubblici e privati. Nessuno è al sicuro dai rischi cibernetici. Se già con la pandemia si era registrato un significativo aumento dei crimini digitali, la guerra in corso tra Russia e Ucraina ha drammaticamente messo la questione "sicurezza informatica" al centro dei riflettori. Pnrr, transizione digitale, cybersecurity, sanità digitale e industria 4.0 saranno al centro di un dibattito che si terrà presso la sala Capitolare del Senato della Repubblica domani, giovedì 3 marzo, alle ore 9, nell'ambito degli Stati generali dell'ingegneria dell'informazione su iniziativa del presidente dell'intergruppo parlamentare inclusione digitale, senatrice Urania Giulia Papatheu, insieme ai colleghi parlamentari dell'Intergruppo ed in collaborazione con il Consiglio nazionale degli ingegneri (Cni). Aprirà i lavori la senatrice Urania Papatheu, presidente Intergruppo parlamentare inclusione digitale e parteciperanno tra i tanti ospiti Mauro Minenna, capo dipartimento per la Trasformazione digitale del Mitd, Armando Zambrano, presidente Consiglio nazionale Ingegneri (Cni), Alessandro Astorino, coordinatore Consiglio

operativo Comitato italiano ingegneria dell'informazione (C3I) e Luisa Franchina, vicepresidente Centro studi Difesa e Sicurezza (CESTUDIS). L'evento sarà trasmesso in diretta webtv su webtv.senato.it.