LE IDEE INCONTRANO LE AZIENDE

GDB IMPRESA 4.0

Arrivano nuovi mondi e portano nuovi rischi Cybercrime, che fare?

In sala Libretti. Scorcio della sala. Tema: «La visione olistica della sicurezza per contrastare il cybercrime»

In sala Libretti l'incontro Fasternet. Le vulnerabilità più diffuse e un senso (pericoloso) di invincibilità

Tecno-formazione

BRESCIA. Arrivano nuovi mondi. Stanno arrivando cose che noi umani normali manco immaginiamo, come recitava l'androide in Blade Runner. La moltiplicazione delle connessioni (già oggi alta) impallidirà non appena partirà il 5G in grado di collegare, controllare, gestire miliardi e miliardi di cose, case, auto, ospedali, fabbriche eccetera eccetera. Ma il 5G è qui, dal prossimo anno sarà pratica corrente. Magnifico, verrebbe da dire.

E così sarà, con ogni probabilità. Con qualche avvertenza. Una su tutte: la sicurezza, quella informatica, la cybersicurezza per battere il cybercrime. Il 2018 è stato un anno terribile: ogni 3 minuti c'è stato un attacco ad aziende grandi e piccole e a noi semplici umani. Serve alzare il livello di sicurezza, serve alzare in primis la consapevolezza. E serve adottare qualche modalità nuova.

«La visione olistica della sicurezza come metodo di contrasto al cybercrime» è stato il titolo che Fasternet ha dato all'incontro di ieri pomeriggio nella nostra sala Libretti. Olistico, quindi globale, complessivo, avendo due-tre punti fermi alla base: che in primis serve maggiore cognizione del problema, che nessuno può garantire sicurezza assoluta, che il 90% degli incidenti è imputabile al fattore uomo e quindi da qui bisogna partire.

«Proteggere i dati è proteggere le persone e questa è una responsabilità sociale»

Giancarlo Turati
Fondatore di Fasternet

Le vulnerabilità. Lo ha ricordato Roberto Bonetti di Ethical Secury. Esperimento: in un tentativo di phishing (abc del cybercrime), durato 4 ore e condotto su 140 aziende, il 20% ha lasciato sul campo un po' di credenziali. Poi c'è il furto di password, e quindi le applicazioni web, le credenziali di default e infine - al primo posto di questa classifica delle vulnerabilità - banalmente: sistemi vecchi, con Pc con vulnerabilità note. Osservazione interessante: se vi fate la domanda su quanto sia fallace il vostro sistema dovete partire da qui, dai punti più deboli. Magari siete bravi in alcune cose, ma se avete Pc vecchi il vostro sistema è vecchio e quindi siete facile preda (se non lo siete già stati).

I Vap, very attack person. Servono tante cose. Miamin Rizzo (di Fasternet) ha parlato di sicurezza perimetrale, di controllo della navigazione e delle sentinelle della fabbrica che sono il contrario dei Vap, i very attack person: gente predisposta ad essere attaccata, abitudinari e senza fantasia nelle password. Campo preferito dei farabutti informatici: le mail. Quel che serve - accanto a tante altre cose - è un firewall umano, un muro di fuoco fatto da gente che sa le cose, che è stata formata ed informata. In altre parole: serve gente in formazione continua e ovviamente un'azienda che abbia la cognizione che questa cosa è indispensabile perchè - e lo ha ricordato Stefano Bodini, sempre di Fasternet - «la sicurezza delle imprese è fatta da persone competenti e consapevoli».

C'è un rischio-caffè. Bodini si è rifatto ad un doloroso fatto di cronaca di qualche tempo fa: una signora prendeva un caffè al tavolino all'esterno di un bar. Un'auto sbanda ed è una tragedia. È difficile prevedere un rischio simile quando vai al bar. Ma è accaduto. E quindi bisogna cercare di abbassare il livello di rischio «perchè se si ferma l'informatica si perde business», cominciando a dividere l'IT dall'OT. Perchè, come già detto, la sicurezza assoluta non c'è. Ma il rischio lo si può dimezzare. // GI. BO.

La prossima uscita di GdB Impresa 4.0 sarà mercoledì 20 marzo

HANNO DETTO

Giancarlo Turati.
«Il primo vero rischio per le aziende è l'assenza di consapevolezza del problema. È un problema perfido perchè chi non ha consapevolezza non si rende neppure conto dei problemi e dei rischi che corre la sua azienda».

Roberto Bonetti.
«Molte vulnerabilità sono banali. In molte aziende ci si può intrufolare con del semplice phishing tramite mail. Ma il problema più grande per le aziende è che hanno - semplicemente - Pc vecchi».

Miamin Rizzo.
«Il 90% degli attacchi arriva in azienda via mail. Bisogna preparare le persone, creare un fire wall umano, una barriera antintrusione che faccia perno su persone competenti e preparate. Questo devono capire le aziende»

Stefano Bodini.
«Non c'è un livello di sicurezza assoluto così come non c'è "LA" soluzione. Ci sono una serie di cose da fare avendo il quadro d'insieme. Ci sono buone pratiche da adottare, ad esempio dividere l'IT dall'OT».

AVVISO AI NAVIGANTI

Giancarlo Turati, fondatore di Fasternet

IL PRIMO RISCHIO È NON AVERE CONSAPEVOLEZZA

Gianni Bonfadini · g.bonfadini@giornaledibrescia.it

C'è un termine, quasi antico, che sorprendentemente si è ripetuto ieri pomeriggio riecheggiando analogo concetto sentito in convegni internazionali: ed è consapevolezza. E' una virtù che pensavamo desueta e che invece nella nuova cassetta degli attrezzi 4.0 bisogna prepotentemente ritirare fuori. «E' il vero vulnus delle nostre aziende. La vera fragilità nascosta e per questo doppiamente perfida», commenta Giancarlo Turati. «Semplicemente e tremendamente le aziende - molte, non tutte per fortuna - non hanno la cognizione di quel che significa sicurezza informatica, sono tutte protese a fare investimenti in macchinari ma si dimenticano, sottovalutano, se ne scordano addirittura, che quelle macchine, quei software, il patrimonio di dati che hanno dentro va difeso. Se i dati sono il vero nuovo tesoro va costruito attorno a loro una difesa. Serve, appunto, la consapevolezza di quel che si ha e quindi urgono investimenti conseguenti. Fra i sei trend che analisti importanti segnalano per chi vuole continuare a fare business, la sicurezza informatica è al primo posto. Poi ci sono i problemi della geopolitica e la significatività della A.I., ma - al primo posto - viene la sicurezza informatica. Chi arriva prima ad avere questa cognizione e quindi, e di conseguenza, chi avvia per primo processi di difesa e controllo ha maggiori garanzie di continuare a fare impresa. Non ha la sicurezza assoluta (questa non la può dare nessuno) ma certamente parte avvantaggiato. Il problema è questo: i dati conteranno sempre più, e quindi sempre più bisognerà alzare difese per la loro integrità».

Se i dati sempre più saranno importanti, è urgente attivare difese adeguate