...ready for the future

Certification for Integrated System Management
ISO 9001:2008 N. AT-13597
ISO 14001:2004 N. 2322
ISO 27001:2013 N. 102
OHSAS 18001:2007 N. 912

ALASCOM

Cyber Security

Alascom, the ideal partner to develop IT/OT solutions based on innovative technologies

Alascom Services Mozambique

www.alascom.it

Alascom Information Technology Middle East L.L.C.

...ready for the future

INDICE

Alascom,
the ideal partner
to develop IT/OT
solutions based
on innovative
technologies

...ready for the future

APT Attack Simulation.mp4

Alascom,
the ideal partner
to develop IT/OT
solutions based
on innovative
technologies

La Cyber security

È un ramo dell'information security e si occupa prevalentemente dell'ambito tecnologico, sviluppando tecnologie e sistemi in grado di rilevare cosa accade e come.

Alascom, the ideal partner to develop IT/OT solutions based on innovative technologies

...ready for the future

Cyber security Focus point

- *Il numero e la complessità degli attacchi informatici è in rapido e costante aumento*
- *Comprovati incident di sicurezza in ambito energetico*
- *Dal 2018 si calcola che le compagnie Oil&Gas spenderanno circa $1.87 bilioni all'anno in Cyber security*

Alascom, the ideal partner to develop IT/OT solutions based on innovative technologies

...ready for the future

Cyber security e Infrastrutture Energetiche

L'aggregazione dei dati, le analisi sui consumi e l'automazione dei controlli,

hanno portato le infrastrutture energetiche a trasportare sempre più dati su reti profibus, ibride/custom o IP.

Tutto ciò porta a riflettere sulla sicurezza del dato e sulla sicurezza e privacy dell'utenza finale.

Alascom, the ideal partner to develop IT/OT solutions based on innovative technologies

...ready for the future

Energia, motore dell'economia moderna

I rischi legati alla cyber security crescono in modo proporzionale a come aumentano a dismisura metodi sempre più sofisticati e frequenti d'attacco.

***Le conseguenze fisiche ed economiche di un attacco a infrastrutture energetiche nazionali possono essere catastrofiche**, questo rende agli occhi del Cracker, l'obbiettivo sfidante e di altissimo interesse.*

Alascom, the ideal partner to develop IT/OT solutions based on innovative technologies

...ready for the future

Energia e Cyber security incident

attacchi noti ad infrastrutture energetiche

2003 , USA Nuclear power plant Malware

«Slammer» rimane attualmente il worm a diffusione più rapida della storia.

Nel 2003 con questo vettore fu attaccato un impianto nucleare in Ohio permettendo di disabilitare per 5 ore il sistema di safety monitoring.

2012, USA Power Generation Human error/virus

I sistemi ICS di una power utility americana furono infettati dal virus noto come «mariposa»; Un tecnico di terze parti intervenuto per una banale manutenzione, utilizzando una chiavetta USB virata per un upload software dei sistemi generò un downtime della intera infrastruttura e portò a ritardare riavvii pianificati per 3 settimane.

2012 ARABIA SAUDITA OIL Company virus

Il Virus denominato «shamoon» fu in grado di infettare circa 30,000 computer della più grande compagnia produttrice di oil e gas del mondo(Saudi Aramco) Molti di questi sistemi rimasero inaccessibili per più di 10 giorni e 85% dell'hardware di proprietà della compagnia andò distrutto; il virus ebbe impatto sulla intera economia nazionale.

Alascom,
the ideal partner
to develop IT/OT
solutions based
on innovative
technologies

...ready for the future

2012 PAESI BASSI Telecommunications Hacking

Un ragazzo di 17 anni fu arrestato per aver violato centinaia di server; i server coinvolti erano gestiti da una compagnia di telecomunicazioni che rivendeva servizi di smart-meter alle utilities.

2013 – 2015 USA e CANADA Power Generation Human error/virus

Una compagnia operante su circa 50 power plant americane e canadesi fu attaccata grazie ad informazioni rubate da un proprio contractor. Gli attaccanti furono in grado di estorcere power plant design critici e password amministrative di sistema.

2014 GERMANIA Manufacturing Hacking

Un gruppo di Cracker attacco il business network di un acciaieria tedesca, causando danni massivi all'intero equipaggiamento industriale, fu il secondo attacco rilevato ad avere effetto sulle infrastrutture fisiche.

2015 UCRAINA Power Grid Hacking / human error

In questo caso l'attaco fu pianificato nei minimi dettagli prima di essere scatenato verso 3 compagnie di distribuzione elettrica causando disservizi su circa 80.000 clienti. Fu il primo attacco noto a causare un totale disservizio di fornitura elettrica. L'attacco avvenne attraverso una campagna di pishing avente come target lo staff IT delle compagnie coinvolte.

Alascom, the ideal partner to develop IT/OT solutions based on innovative technologies

...ready for the future

2015 SUD COREA Nuclear power plant hacking

Le società Korea Hydro e la Nuclear Power Co. subirono una serie di attacchi atti a causare malfunzionamenti dei reattori nucleari; l'attacco permise di accedere a documenti non classificati.

2016 ISRAELE Public sector Power Grid Malware / human error

Un dipendente dell'autorita elettrica israeliana fu il vettore di un attacco di tipo phishing, il quale infettò una parte dei computer aziendali presenti in rete con dei Malware. Power grid non fu interessata da questo attacco ma questo porto comunque l'autorità elettrica a 2 giorni di lavoro per riportare il tutto alla normalità.

2015 AUSTRALIA Public Sector Hackin / virus

Attaccanti violarono il Maitland office del dipartimento risorse ed energia in New South Wales. Gli attaccanti si interessarono a violare progetti in corso del dipartimento e link che garantivano accesso a documenti governativi classificati.

Alascom, the ideal partner to develop IT/OT solutions based on innovative technologies

...ready for the future

SCADA security

La SCADA security è quel ramo della cyber security nato per controllare e difendere ambienti ICS, fornendo analisi su protocolli industriali proprietari e open (profibus,modbus etc)

Esistono ormai parecchie compagnie in grado di rilevare attraverso sonde out-of-band o in-line anomalie e cambiamenti all'interno delle infrastrutture SCADA appoggiandosi a sistemi cognitivi, predittivi e di machine learning.

Alascom, the ideal partner to develop IT/OT solutions based on innovative technologies

Alascom vision

«Si necessità della realizzazione di una visione integrata del rischio tra funzioni di controllo e strutture specialistiche che permetta di presidiare il rischio informatico nella gestione dei processi IT.

L'integrazione deve avvenire in modo strutturato lungo tutti i principali processi IT mediante l'adozione di presidi organizzativi, processi e soluzione tecnologiche che possano permettere di monitorare l'intero perimetro delle componenti ICT/ICS e distinguerne l'impatto/ criticità per il business.

L'analisi del rischio informatico diventa uno dei driver principali su cui basare l'evoluzione del proprio sistema informativo di riferimento.»

Alascom,
the ideal partner
to develop IT/OT
solutions based
on innovative
technologies

...ready for the future

Utopia ?

Tutte le parti interessate
(governi, compagnie finanziarie, energetiche, industriali e tecnologiche)
dovrebbero lavorare e collaborare sulle 4 aree ritenute vulnerabili:

- *Fattori tecnici e umani*
- *Controllo delle informazioni e dello sharing di esse*
- *Assessment e quantificazione periodica dei rischi*
- *Definizione di standard e best practice*

Alascom,
the ideal partner
to develop IT/OT
solutions based
on innovative
technologies

...ready for the future

Normative Europe ed Italiane

Prossima scadenza Maggio 2018

Alascom,
the ideal partner
to develop IT/OT
solutions based
on innovative
technologies

...ready for the future

Direttiva NIS parlamento europeo

- *Miglioramento delle capacità di cyber security dei singoli Stati dell'Unione*
- *Aumento del livello di cooperazione tra gli Stati dell'Unione*
- *Obbligo per gli operatori di servizi essenziali e dei fornitori di servizi digitali di adottare un approccio basato sulla gestione dei rischi*
- *Ciascuno Stato membro dovrà anche designare un'apposita autorità che funga da punto di contatto per gli scambi internazionali, dotarsi di una strategia cyber e costituire uno o più CERT/CSIRT (Computer Emergency Response Team)*

Alascom,
the ideal partner
to develop IT/OT
solutions based
on innovative
technologies

...ready for the future

“Misure minime di sicurezza ICT per le pubbliche amministrazioni” Agid Gazzetta Ufficiale

- *Direttiva NIS applicata a livello nazionale*

Alascom,
the ideal partner
to develop IT/OT
solutions based
on innovative
technologies

...ready for the future

Nuovo Regolamento europeo per la protezione dei dati personali (GDPR)

- *In Italia esiste già legge sulla privacy stringente e molto simile al GDPR, è atteso ancora pronunciamento del garante su pochi casi ambigui.*
- *Da sottolineare essendo introduzione completamente nuova: va menzionato l'obbligo, a carico di chiunque gestisca dati personali altrui, di notificare alle competenti autorità ogni violazione degli stessi.*

Alascom, the ideal partner to develop IT/OT solutions based on innovative technologies

Si consiglia la lettura del framework nazionale di cyber security :

http://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf

Alascom,
the ideal partner
to develop IT/OT
solutions based
on innovative
technologies

...ready for the future

Manuel.alessi@alascom.it

contacts@alascom.it

Thank You

www.alascom.it