SECURITATEA CIBERNETICA IN MEDIUL INDUSTRIAL

energynomics.ro, BUCURESTI
07.02.2018

Power & Automation

Engineering & Consulting

Substation Automation & Protection Systems

Process Control & Electrical Automation

IT, Telecom & Cyber Security

7

industries:

Power Generation, Power Transmission and Distribution, Water, Oil & Gas, Steel, Food & Beverages, Chemicals

4

offices:

Bucharest, Resita, Saudi Arabia (Al Jubail) and Australia (Melbourne)

40

Projects

on SCADA and control, for power generation, power T&D, steel and diary industries

50%

Of revenue

From international projects

3.500+

IEDs

integrated and monitored through our solutions

3

EMS-SCADA Dispatch Centers

Designed and implemented by ENVO Group

500.000+

Data collection points

aggregated

100+

Equipment providers

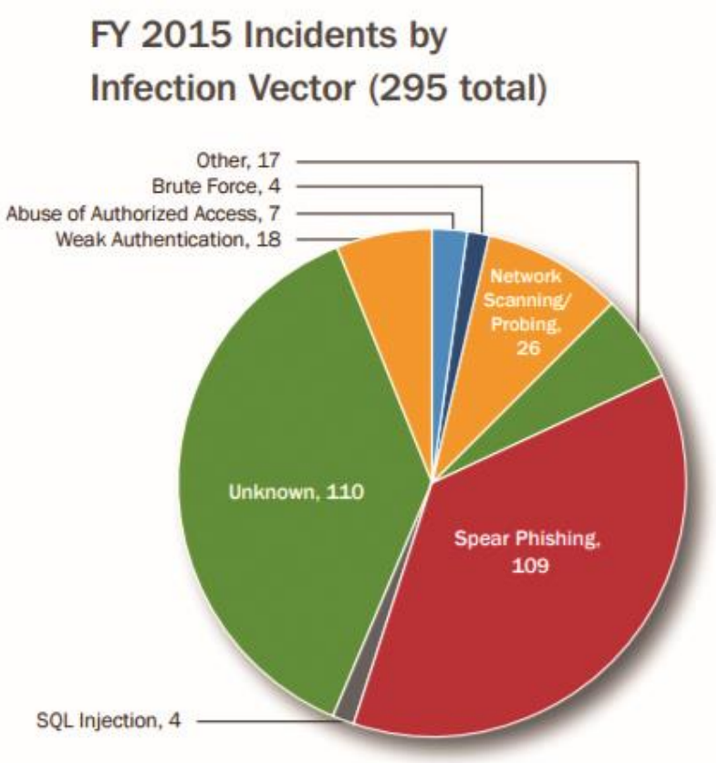
Integrated in ENEVO's dispatch and automation solutions

Particularitati ale sistemului energetic raportate la securitatea cibernetica

- Criticalitate
- Inertie tehnologica si echipamente legacy
- Schimbari de structura pe aceeasi infrastructura: operare centralizata – retea extinsa – operare descentralizata
- Obiective izolate si securizate fizic vs obiective online
- IoT introduce noi vectori de atac si noi variabile in formulele de fiabilitate

Lipsa unei imagini de ansamblu

- Sistemele de Control Industrial (SCI) nu sunt de obicei prevazute cu solutii de protectie impotriva amenintarilor cibernetice.
- Lipsa acestora genereaza si o lipsa de informatii vitale pentru a intelege atat expunerea (numarul si tipul de echipamente infectate) cat si noile tehnici de atac folosite.
- Fara aceasta baza, reactia defensiva este puternic ingreunata, incidentele sunt descoperite greu si tarziu.
- Echipa de raspuns la incidente cibernetice industriale a Departamentului Apararii al SUA (ICS-CERT) publica anual date privind numarul de incidente pe care le analizeaza.
- In fiecare an, raportul celor de la ICS-CERT indica "metode necunoscute" ca principal vector de atac.
- O analiza a bazei de date publice VirusTotal estimeaza ca, in prezent, intre 3.000 si 4.500 de organizatii industriale au sistemele de control infectate.



AMENINTARILE

2010: Stuxnet

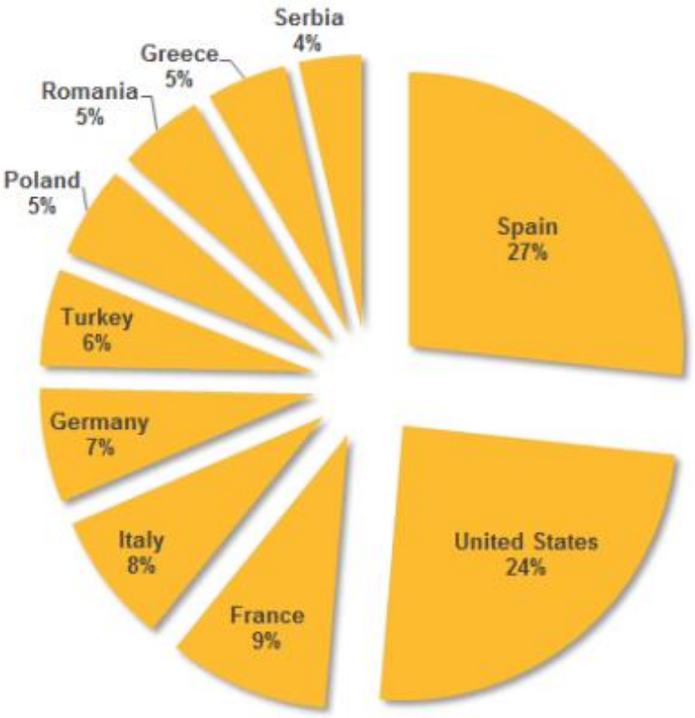
- Unde: IRAN
- Sistemul tintit:
  - Instalatia de imbogatire a Uraniului din Natanz
  - PLC-uri Siemens S7-315 echipate cu cate 6 module CP-342-2, fiecare modul fiind conectat la 31 de VFD-uri tip Vacon sau Fararo Paya
- Vectorul de atac: stick USB infectat introdus de unul dintre cei 5 subcontractori ai instalatiei
- Impact: IAEA (International Atomic Energy Agency) estimeaza ca 1000 de centrifuge au fost scoase din uz
- Esential de retinut:
  - Primul malware dedicat unui sistem de control industrial
  - Creatorii sai au avut o foarte buna intelegere a procesului industrial
  - **Atac fara acces direct la retea (RETEA IZOLATA)**
  - Au infectat intai organizatii care interactionau cu tinta (atac pivot)
  - Capabil sa modifice si sa mascheze linii de cod in PLC-uri Siemens

2013: Dragonfly/HAVEX

- Unde: SUA si Europa
- Sistemele tintite:
  - Retelele electrice si instalatiile petrochimice
  - Echipamentele care comunica prin porturile TCP 44818 (Omron, Rockwell Automation), 102 (Siemens) si 502 (Schneider Electric)
- Vectori de atac: site-urile producatorilor de echipamente si mailuri cu PDF-uri infectate

(atacuri de tip spear phishing)

- Impact: > 2,000 siteuri (1,000 de companii din sectorul energetic din 84 de tari)
- Esential de retinut:
  - S-a folosit de o functionalitate a protocolului industrial OPC pentru a scana retelele infectate
  - Probabic cea mai mare campanie de spionj cibernetic industrial
  - Nu a cauzat perturbari sesizabile ale proceselor industriale sau distrugeri de echipamente ci numai exfiltrare de date

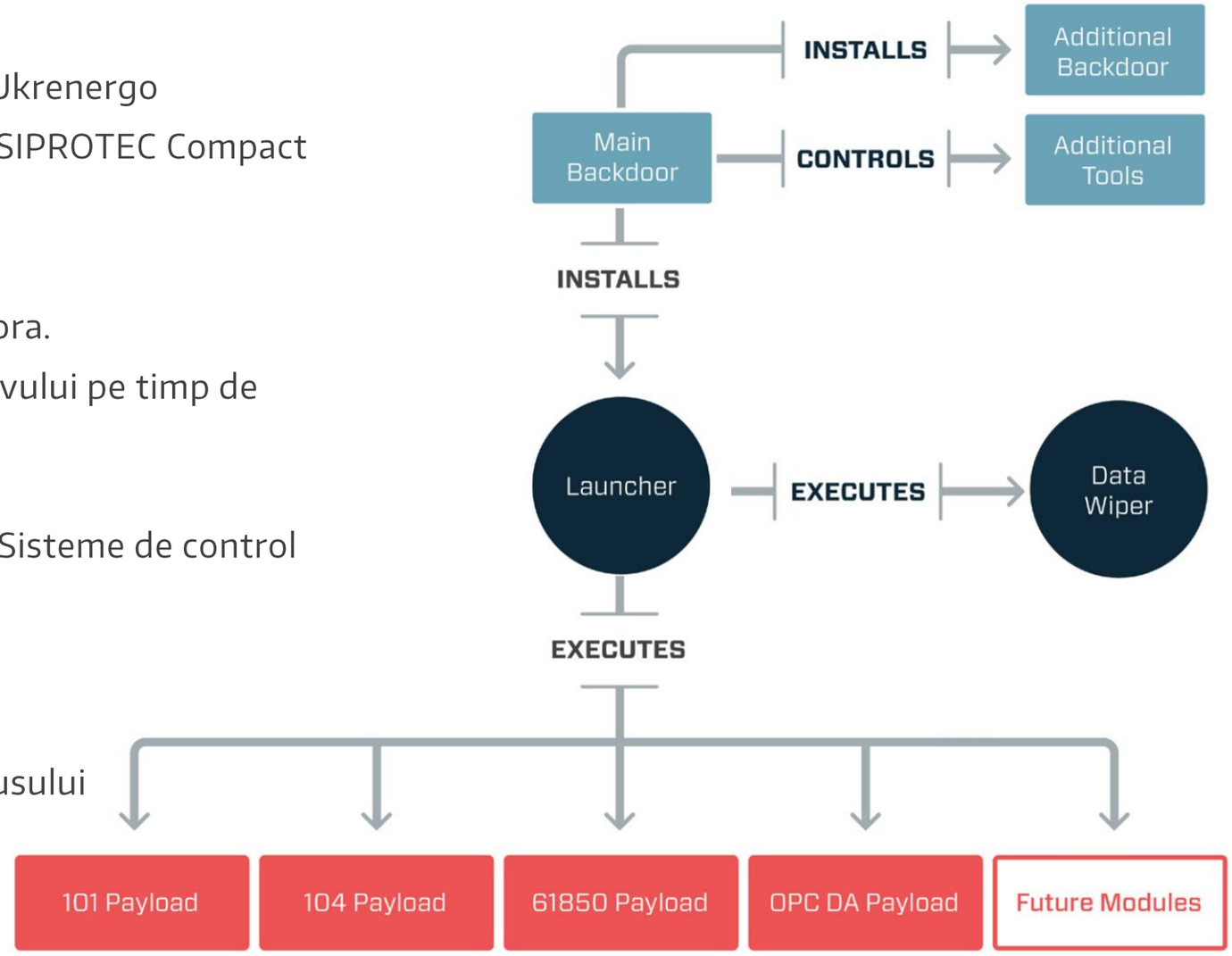


2015: Blackenergy 3

- Unde: Ucraina
- Sistemele tintite: 3 companii de distributie de energie
- Vectorul de atac: mailuri cu atasamente infectate (spear-phishing)
- Impact:
  - **7 statii de 110 kV** si **23 de statii de 35 kV deconectate**
  - **225,000+ consumatori** fara energie electrica pentru **~6 ore**
- Esential de retinut:
  - Recunoscut ca primul atac cibernetic care intrerupe functionarea unei retele electrice
  - Distrugerea unor convertoare de semnal (serial-ETH) prin update de firmware corupt
  - A cauzat pierderea controlului de la distanta a echipamentelor. Pentru unele statii, pentru mai bine de un an.
  - A intors impotriva retelei modul de functionare al sistemelor ce deservesc statiile eletrice

2016: Crashoverride

- Unde: Ucraina
- Sistemul tintit:
  - Statie de transformare din Kiev detinuta de Ukrenergo
  - Relee de protectie Siemens SIPROTEC 4 and SIPROTEC Compact
- Vector de atac: momentan necunoscut
- Impact:
  - A deconectat de la retea 200 MW pentru ~1 ora.
  - Asigurau ~1/5 din consumul de energie al Kievului pe timp de noapte
- Esential de retinut:
  - Framework modular dezvoltat special pentru Sisteme de control industrial
  - Primul malware creat special pentru a ataca retele electrice
  - Atacul pare mai degraba un test de concept, nu unul care sa fi folosit toate capacitatile virusului

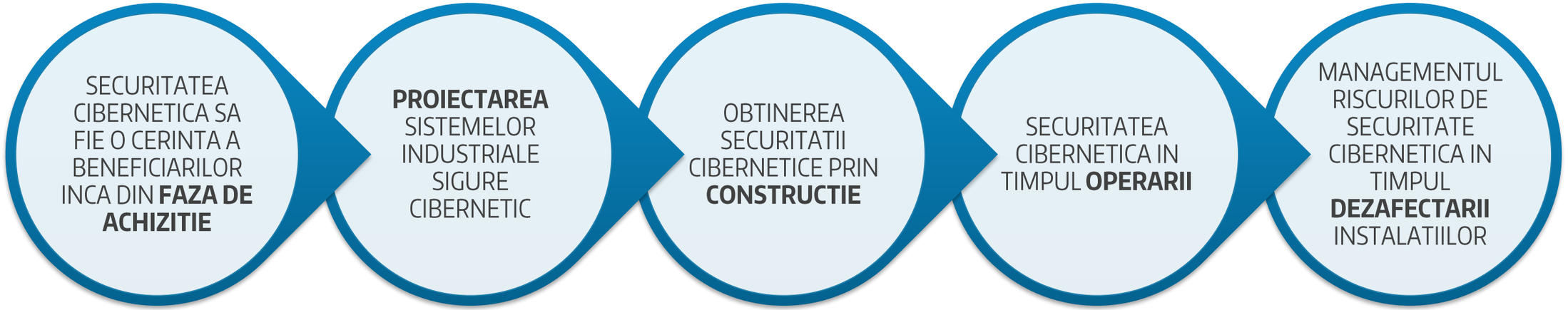


2017: Trisis

- Unde: Orientul Mijlociu
- Sistemul tintit:
  - Sistemul de siguranta a procesului - Triconex System (Schneider Electric)
  - Mai exact, procesoarele Tricon 3008 bazate pe o arhitectura PowerPC (echipament legacy);
- Vetorul de atac:
  - Acces de la distanta pe o statie de lucru de inginerie ce putea modifica sistemul
- Impact:
  - Inchiderea completa instalatiei
- Esential de retinut:
  - Primul malware gandit special sa atace sisteme de siguranta;
  - Facilitat de rele practici in mentenanta echipamentelor (cheia de control lasata in modul “programare”)
  - In ultima instanta, sistemul a functionat: a simtit ceva in neregula si a inchis fabrica, inainte ca restul comenzilor sa poata fi date
  - Desi atacul nu este scalabil, o parte din codul sursa este la liber pe internet, putand fi folosit ca punct de plecare pentru viitoare atacuri impotriva sistemelor de siguranta a proceselor industriale https://github.com/ICSrepo/TRISIS-TRITON-HATMAN

Ce putem face

Securitatea cibernetica, parte din ciclul de viata al sistemelor de control industrial



- Cooperare strategica a producatorilor, furnizorilor si integratorilor de echipamente/sisteme implicati in lantul tehnologic
- Contractele sa includa si cerinte clare de Securitate cibernetica

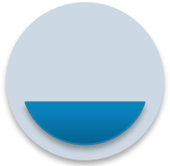
- Implicarea in proiectare a unui Expert in Securitate Cibernetica a Sistemelor Industriale (SME)
- Conceperea unor programe de training si constientizare pentru personal
- Introducerea cerintelor de Securitate cibernetica in specificatiile de proiectare
- Evaluarea proiectarii sistemelor de Securitate cibernetica

- Politici de Securitate (e.g. testarea firewallurilor, liste de permisiuni si software anti-malware)
- Testarea capacitatilor si uneltelor pentru recuperarea dupa "dezastru"
- Testarea patchurilor si updateurilor software
- Testarea rezistentei sistemului (de ex., teste de hacking)
- Monitorizarea sistemului (de ex, salvarea si analiza logurilor de sistem).

- Desemnarea unui responsabil de Securitate cibernetica
- Implementarea programelor de training si constientizare pentru personalul operator
- Operarea si mentenanta echipamentelor dedicate securitatii
- Securizarea modalitatilor de modificare a parametrilor de proces

- Distrugerea sau stocarea in siguranta a echipamentelor/datelor de process.

Masuri



Evalueaza:

- Evalueaza Sistemul si Identifica Echipamentele Critice
- Stabileste Zonele procesului & comportamentele permise in fiecare sau intre ele
- Analizeaza riscurile fiecarei zone
- Stabileste specificatii detaliate de Securitate

Implementeaza

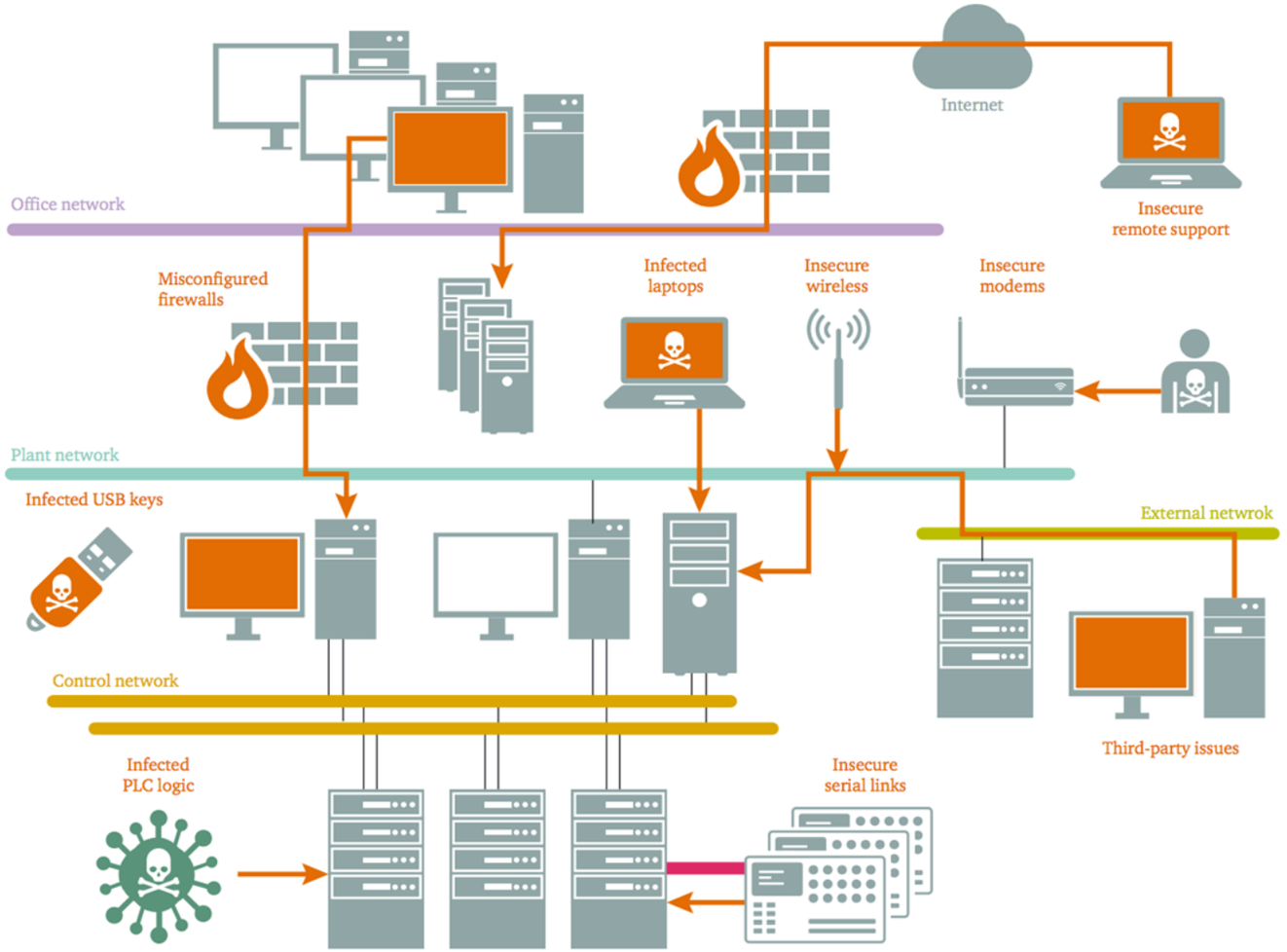
- Proiectare de detaliu a sistemelor de Securitate Cibernetica
- Validarea proiectarii
- Implementarea sistemului
- Validarea implementarii (teste de fabrica si in teren)

Mentine

- Mentine securitatea (instalarea de patch-uri, update antivirusi etc)
- Monitorizeaza sistemul cu solutii dedicate (SIEM, IDS etc.)
- Evalueaza periodic sistemul si politicile de lucru
- Ramai la curent cu cele mai recente bune practici
- Inlocuieste si scoate din uz in mod sigur echipamentele depasite

Prevenție

- Modificarea mindset-ului
- Dezvoltarea competențelor interdisciplinare
- Includerea securității cibernetice din fazele de proiectare, inginerie și licitație/ofertare
- Actualizarea constantă a infrastructurii
- Monitorizarea activă a infrastructurii
- Cooperarea cu toți actorii implicați în securitate cibernetică
- Viziune unitară asupra securității cibernetice
- Cod de bune practici
- Reglementare



Multumesc pentru atentie!

Romania Office

Address: 9 Piata Pache Protopopescu
Bucharest, Romania
Phone: +40 371 017 242
Fax: +40 372 258 353
Email: romania@enevogroup.com

Saudi Arabia Office

Address: Al Jubail 31961, Support Industrial Zone,
Kingdom of Saudi Arabia
Phone: +966 013-3408324
Fax: +966 013-3408322
Email: ksa@enevogroup.com

Australia Office

Address: Level 2, 172-192 Flinders Street, Melbourne, Australia
Phone: +61 414 384 430
Email: australia@enevogroup.com

www.enevogroup.com