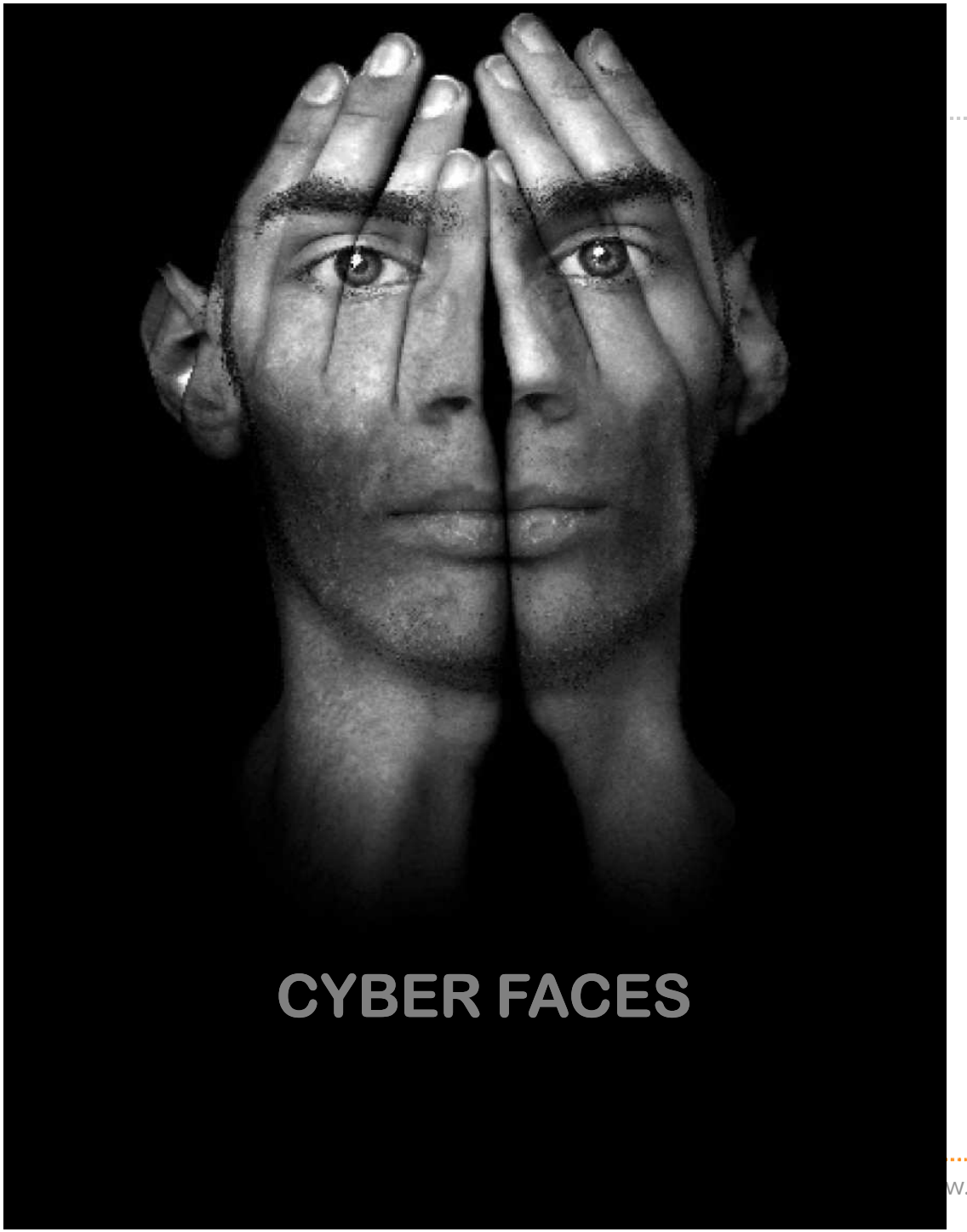


CYBERWAR

Ivan Bütler

Compass Security AG

www.csnc.ch

Cyber War – define it!

RSA Breach

WikiLeaks

Click here to make a secure submission

LOCKHEED MARTIN

Definition of a traditional conflict/war

War is a state of organized, armed and often prolonged conflict carried on between states, nations, or other parties. Such a conflict is always an attempt at altering either the psychological or material inter-group relationship of equality or domination between such groups

When do we name a conflict as war?

War is an act of violance with direct impact to our society, social live, wealth, enonomy and health.






Definition: „Cyber War“

Cyber War is an act of violance in the cyber space with direct impact to our society, social live, wealth, enonomy and health.

This war is performed by cyber troops

Problem: Hard to define the difference to cyber espionage or cyber crime

Hacking Methodology

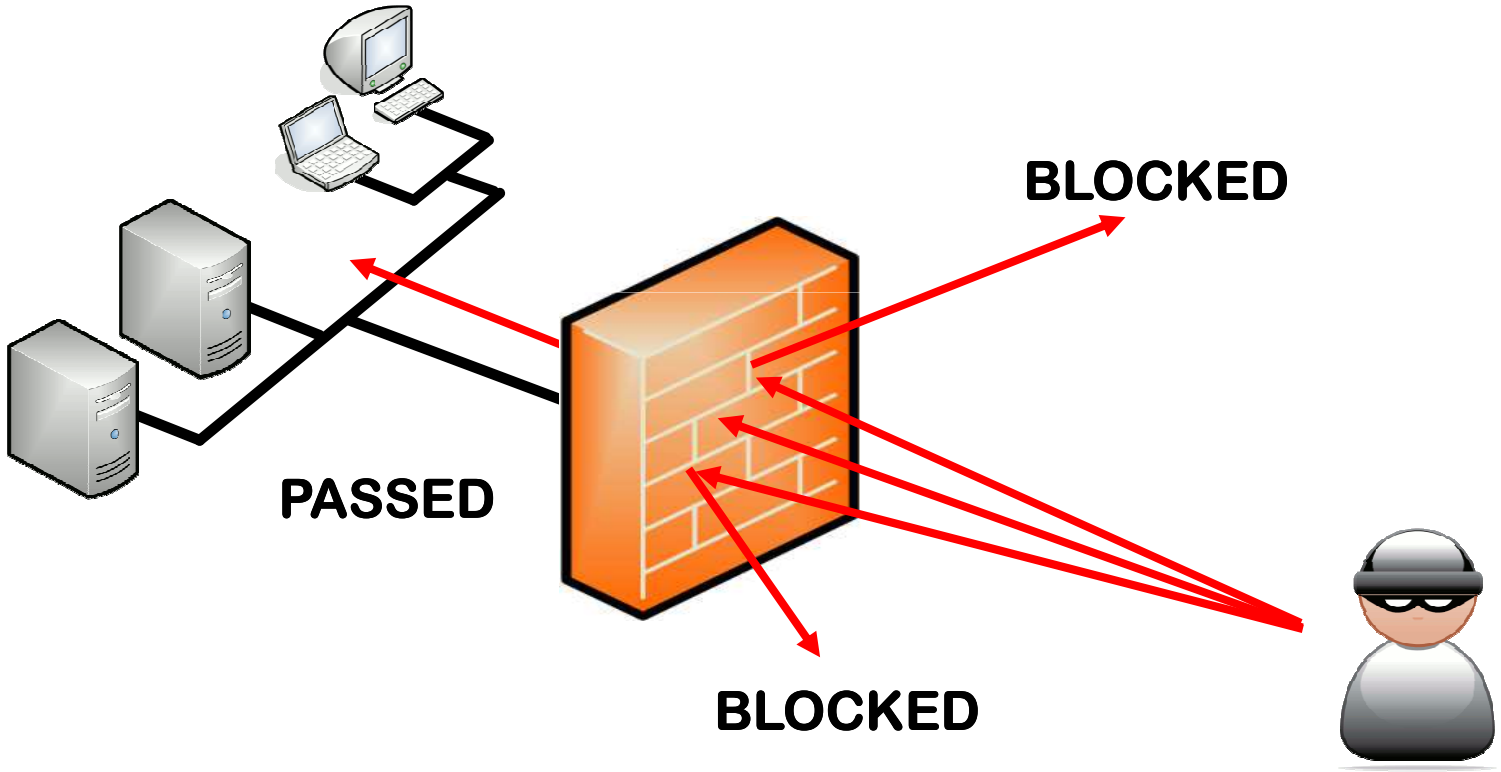
HOW TO GAIN UNAUTHORIZED ACCESS INTO FOREIGN COMPUTERS OR NETWORKS

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

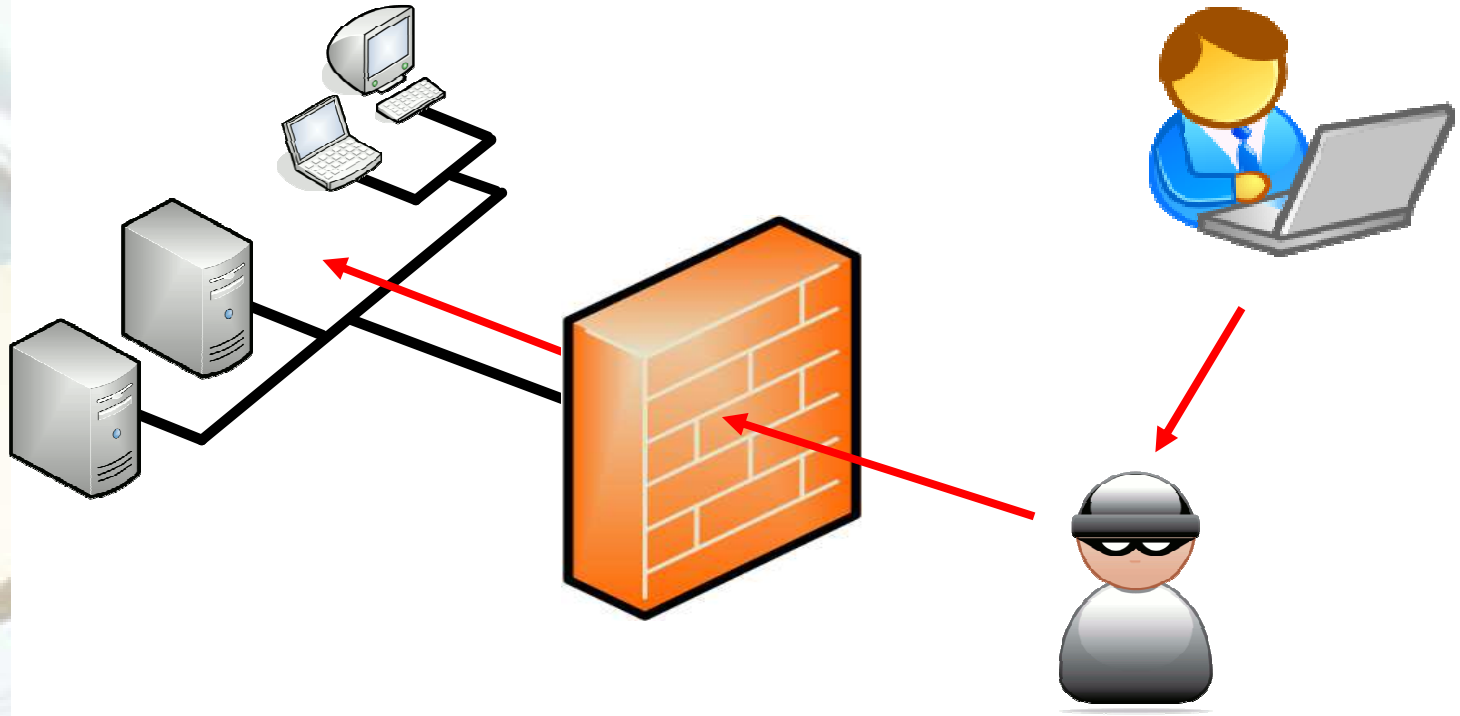
Direct Attack

Server Exploitation



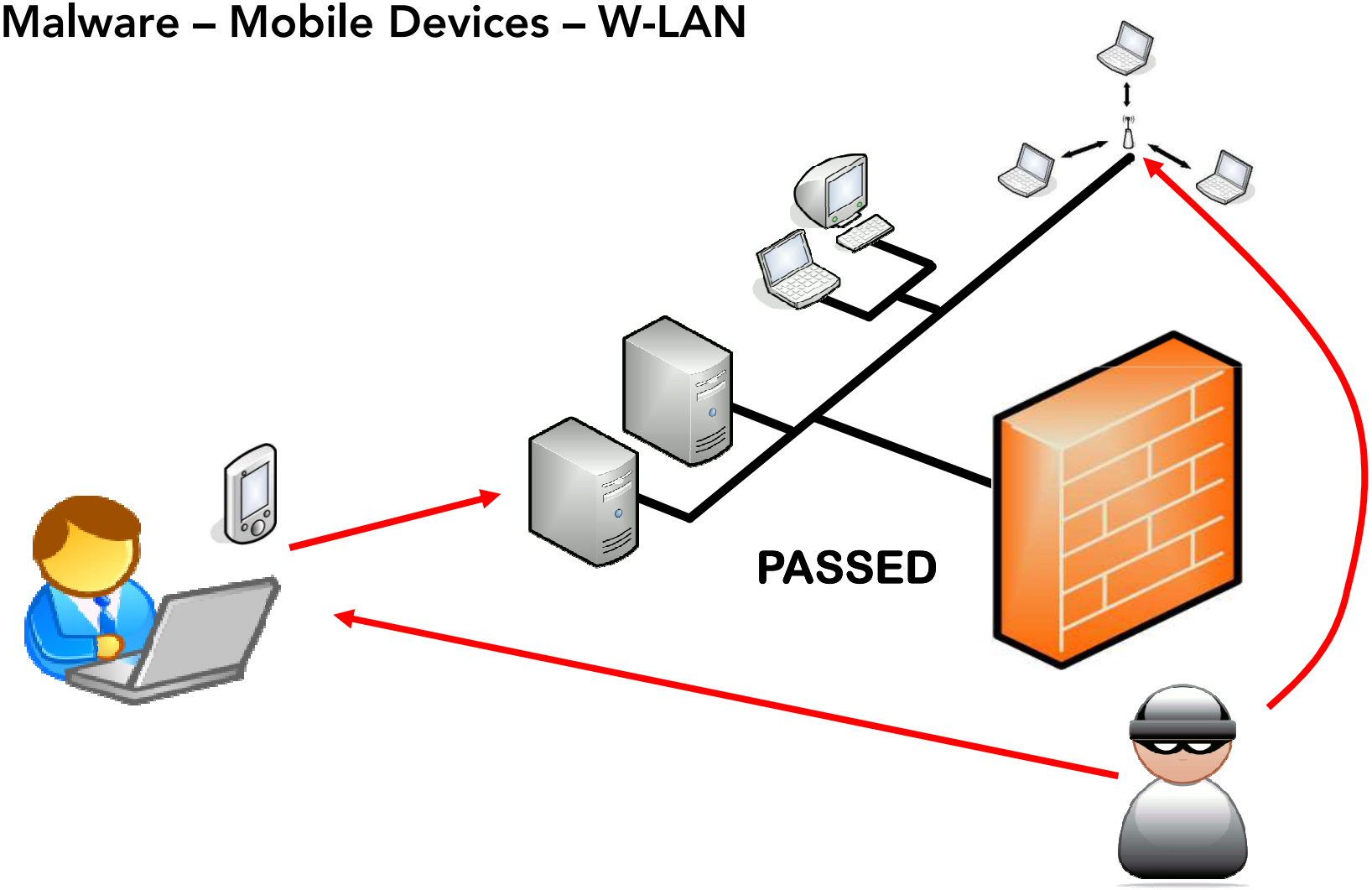
Man in the Middle

Man in the Middle – Phishing

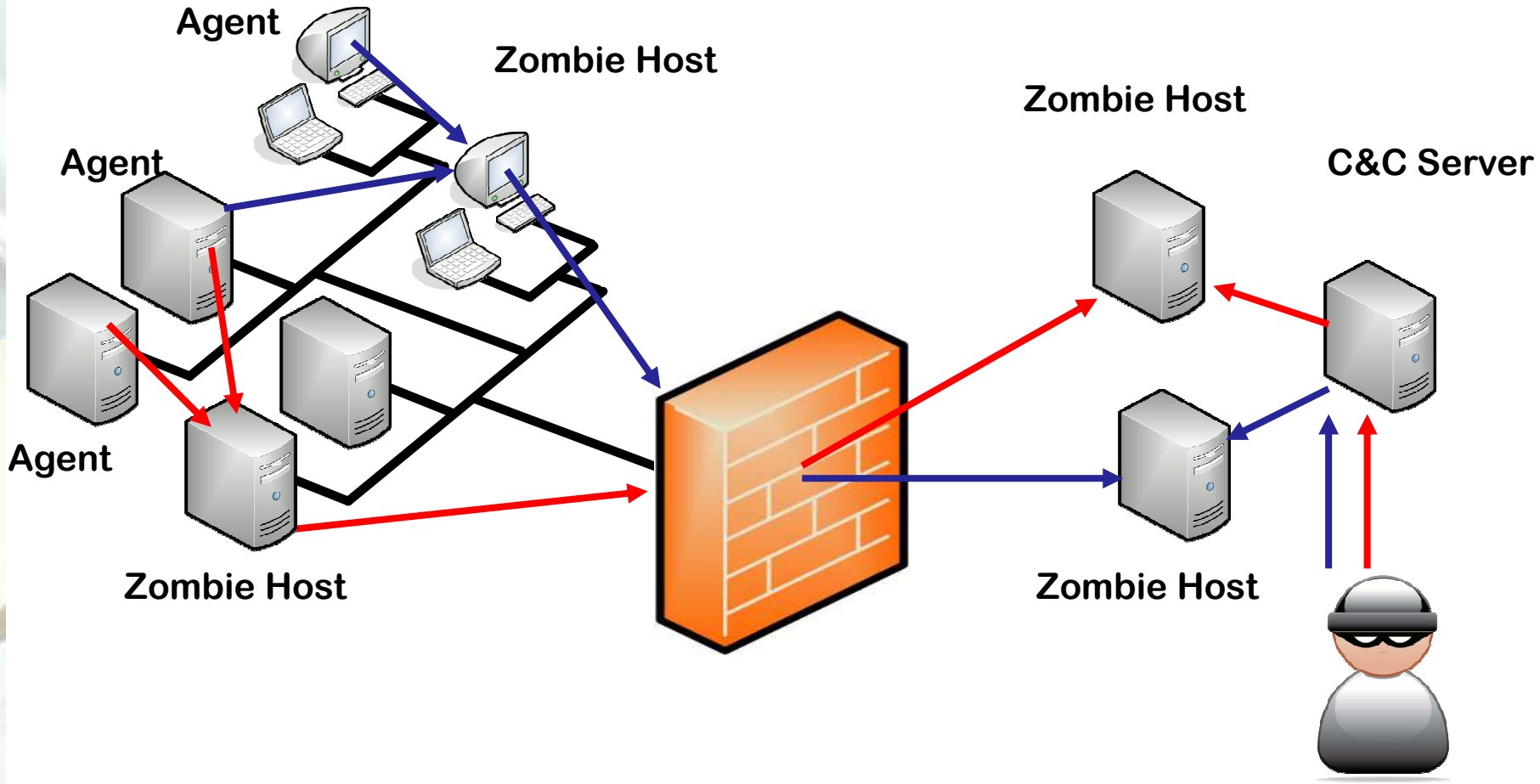


Indirect Attack – Virus and Trojan

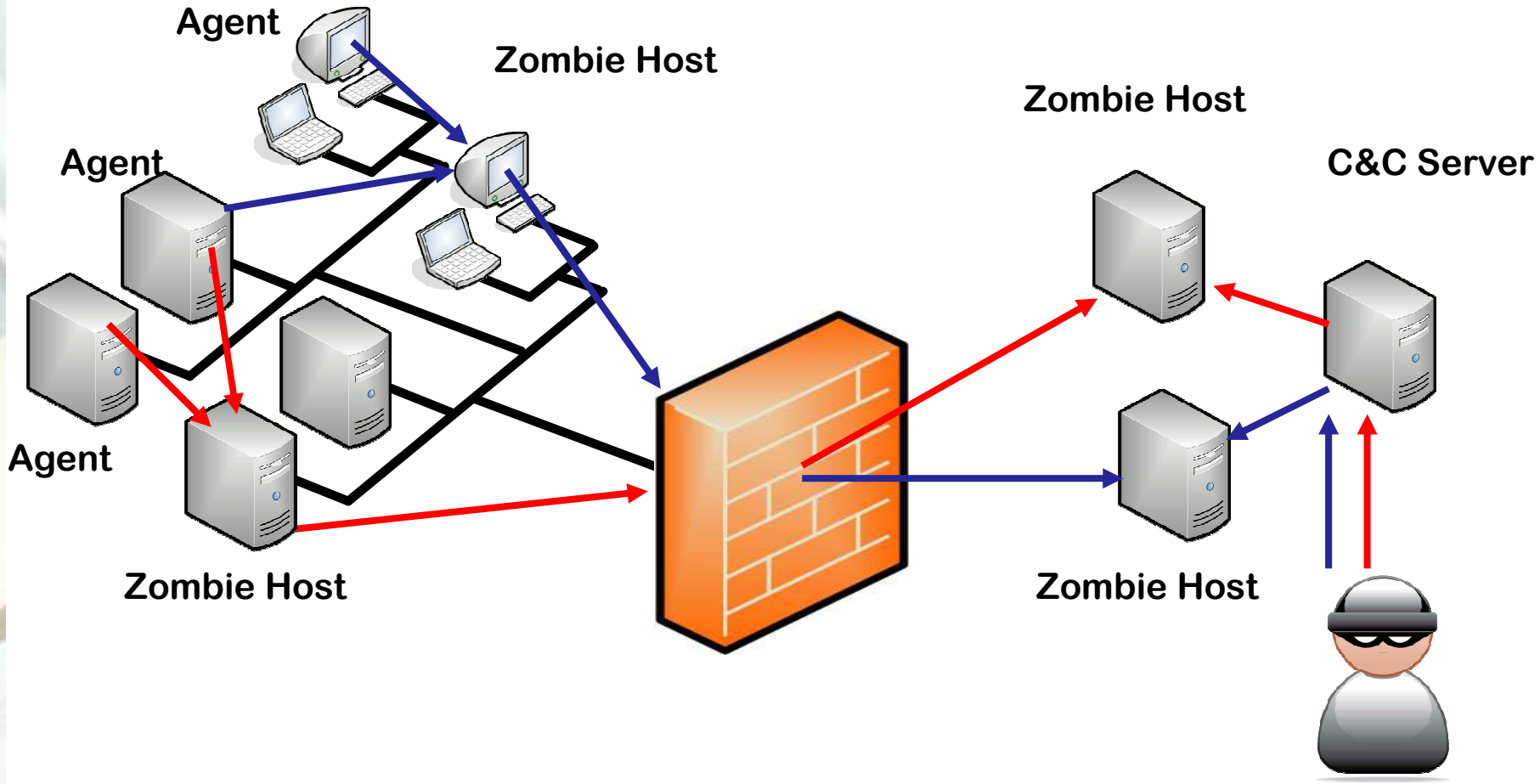
Malware – Mobile Devices – W-LAN



Advanced Persistent Threat (APT)



Advanced Persistent Threat (APT)



APT == Cyber Warfare Framework

Vulnerability Research

Exploit Development

Packer Polymorphic Anti-Reverse

Infection Department

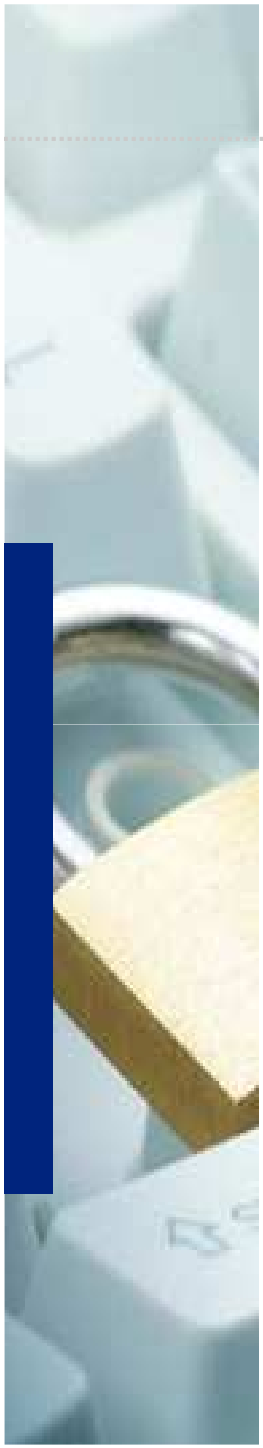
Persistence Layer (Hiding / Rootkit)

C&C Mission Control

High Availability

Crypto Development

Update Mechanism



Targets of a cyber war

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Critical Infrastructures - Switzerland

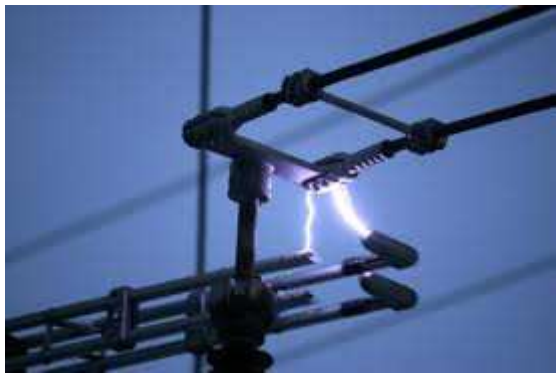
http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/kritische_infrastrukturen.html

1) Cyber Attacke: Administration

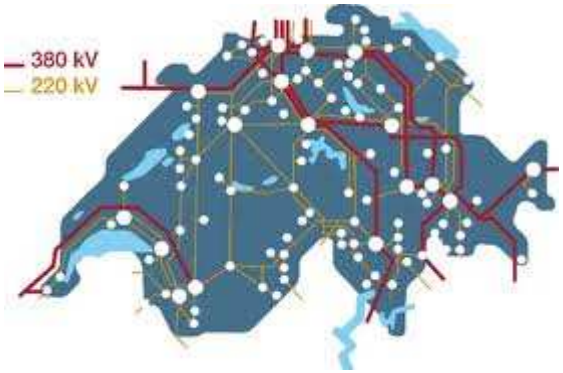
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für auswärtige Angelegenheiten EDA
Département fédéral des affaires étrangères DFAE
Dipartimento federale degli affari esteri DFAE
Departament federal d'affars exteriurs DFAE

2) Cyber Attack: Energy Industry



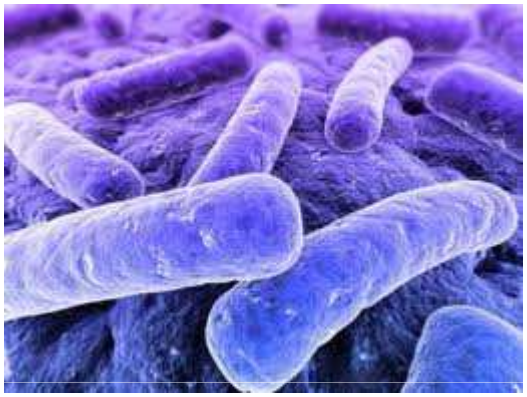
swissgrid

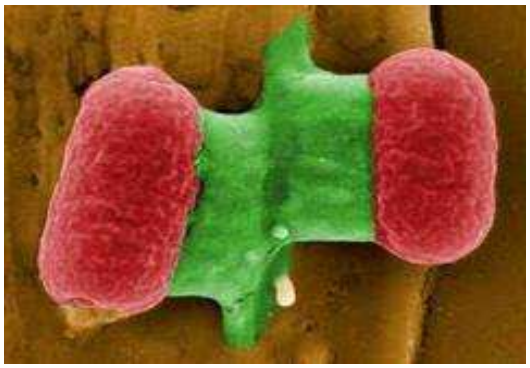


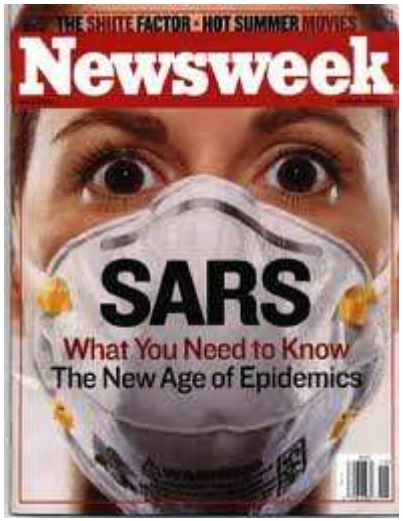
3) Cyber Attacke: Recycling

4) Cyber Attack: Finance

5) Cyber Attack: Health







7) Cyber Attack: IT & Communication

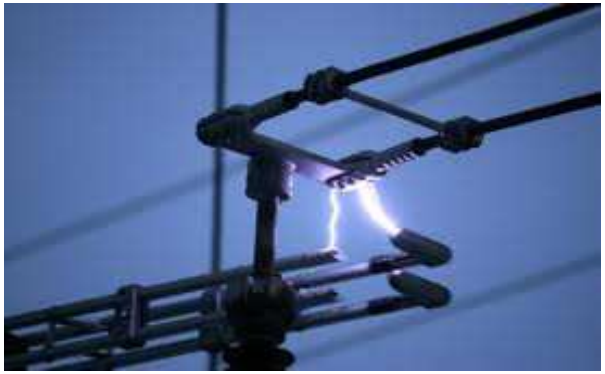
8) Cyber Attack: Food

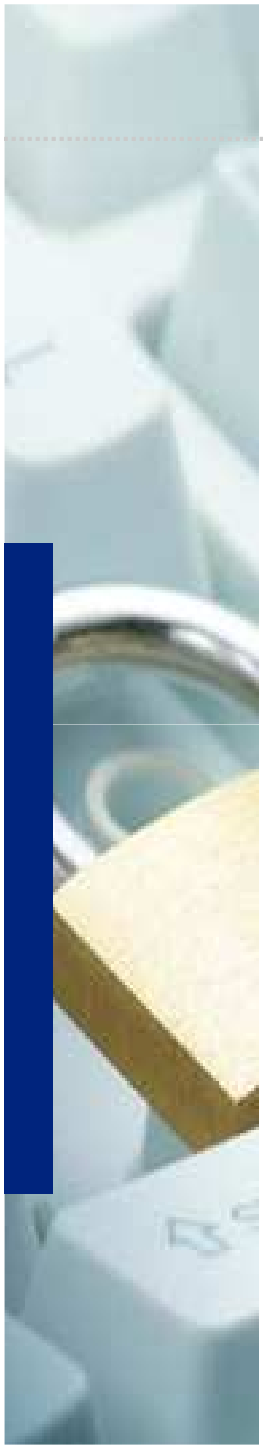
9) Cyber Attack: Public Security

10) Cyber Attack: Transport

Hacking Trends

Hacking Trends





How Governments respond

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

USA – Cyber is new domain of operation

Land

Sea

Air

Space

Cyber

Cyber Troops

USA – Cyber is new domain of operation

On June 23, 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command to establish USCYBERCOM.

GEN Keith B. Alexander
United States Army

Director of NSA and Commander of Cybercom

http://www.defense.gov/cyber

USA: Cyber Command

USA - Act of War (May 31, 2011)

ACT OF WAR

The Pentagon's forthcoming cyber warfare strategy will reframe cyber attacks as possible acts of war, which would allow the US to respond to certain attacks on critical systems with force. US government and military systems have been facing cyber attacks from foreign powers more at least eight years. Attackers have stolen sensitive information, including data about the F35 fighter.

Germany – NCAZ

De Maizière informs about NCAZ

Am 1. April 2011 wurde das neue "Nationale Cyber-Abwehrzentrum" (NCAZ) in Betrieb genommen, ein "Nationaler Cyber-Sicherheitsrat" (NCS) koordiniert Schutzmaßnahmen und Netzpolitik

Switzerland?

Kurt Nydegger

cyberdefense@gs-vbs.admin.ch

Herr Div. Kurt Nydegger wird am 10. Dezember 2010 vom Bundesrat mit der Betreuung des Projektes Cyber Defense und der Entwicklung einer „Nationalen Strategie für Cyber Defense“ beauftragt.

Ende August wird das Dokument soweit gediehen sein, dass es in eine umfassende Vernehmlassung gehen kann.

Unmittelbar nach der Genehmigung durch den Bundesrat im Dezember 2011 werden wir mit der Umsetzung der entschiedenen Massnahmen beginnen.

Recommendation

Take your responsibility

My recommendations for the state

Früherkennung & Abwehr

Bereitstellung von Resourcen / Wissen

Ausbau von MELANI Kapazität

Vernetzung mit andern Ländern / Partnern

Bereitstellung von MIL-CERT / Armee Kapazität

Gesetzliche Rahmenbedingungen CyberWar definieren

Das implementierte Cyber Defense muss beübt werden – Manöver – analog zum US Cyber Storm

My recommendations for a company

Wiedergeburt des todgesagten IDS/IPS

Präventive Einheit mit 7x24h Support

Jedes Unternehmen ist primär selbst verantwortlich für die Abwehr

Der Staat ist die Second Line of Defense und der Vermittler / Supporter

Etablieren Sie Ihre Company Cyber Defense Strategie

Business Continuity Management

Thank you!

Compass Security AG

Compass Security AG
Werkstrasse 20
P.O. Box 2037
CH - 8645 Jona SG

Tel. +41 55 214 41 60
Fax +41 55 214 41 61

team@csnc.ch
www.csnc.ch