CYBER THREATS AND SECURITY MEASURES
INTRODUCTION TO C-CURE

ESTABLISHED IN 1993
SPECIALISED IN CYBERSECURITY
DANISH AND INTERNATIONAL PARTNERS AND SECURITY SPECIALISTS
INDEPENDANT CONSULTANCY, SERVICES, SOLUTIONS AND SUPPORT
AWARENESS TESTS AND AWARENESS TRAINING
MEMBER OF;
• DANISH INDUSTRY (DI)
• DI SECURITY ADVISORY PANEL
• DI’S DIGITAL MENTOR TEAM
• THE ADVISORY BOARD AT THE DANISH POLICE NC3 SKYT
THE INTERNET

NO NATIONS
NO BORDERS
NO GODS
NO MASTERS

FREEDOM OF;
SPEECH
EVOLUTION
INVENTIONS
COMMUNICATION
DEVELOPMENT
DISRUPTION

BUT ALSO FREEDOM OF;
INTERRUPTION
CHILD PORNOGRAPHY
HACKING
THEFT
ESPIONAGE
CYBERWAR
HYPING THE THREATS

NEWS MEDIA AND SECURITY VENDORS TENDS TO "HYPE" MALWARE OUTBREAKS

RUMORS AND INFORMATION ABOUT ATTACKS RUN LIKE A RIOT, WITH INCORRECT ALERTS ABOUT "MASSIVE ATTACKS", DESPITE THE FACT THAT ONLY A FEW COMPANIES ARE HIT NATIONALLY.
THE NEWS IS THAT THERE IS NO NEWS

WHY PATCHING? WHY NOT PROPER PROGRAMMING?

FROM A DOTALOGICAL POINT OF VIEW THE PROBLEMS HAVE BEEN THE SAME DURING THE LAST 40 YEARS;

• BUFFER OVERFLOWS

• LACK OF INPUT VALIDATION

• STANDARD PASSWORDS INSTEAD OF PASSPHRASES AND WITH NO INFORCED CHANGES

• UNDOCUMENTED BACKDOORS (EG. ON IOT DEVICES, PRINTERS ETC.)

• NEGLIGENCE TO ENSURE PRIVACY BY DEFAULT AND PRIVACY BY DESIGN
THE NEWS IS THAT THERE IS NO NEWS

Users want freedom and access to as many services, informations and apps as possible for ease of use and user satisfaction, it administrators allow the users;

- Open access to ports
- Open access to services
- Open access to information
- Local administrator rights
THE EMERGING LANDSCAPE OF CYBERTHREATS

BBC HIRED THE SECURITY COMPANY “CYBERREASON” TO CARRY OUT A CYBER SECURITY TEST.

SERVERS WERE GIVEN REAL PUBLIC IP ADDRESSES AND OTHER IDENTIFYING INFORMATION THAT ANNOUNCED THEIR PRESENCE ONLINE.

ABOUT 71 MINUTES AFTER NEW SERVERS WENT ONLINE THEY WERE VISITED BY AUTOMATED ATTACK TOOLS

17% OF THE ATTACK BOTS WERE SCRAPERS THAT SOUGHT TO SUCK UP ALL THE WEB CONTENT THEY FOUND

37% LOOKED FOR VULNERABILITIES IN WEB APPS OR TRIED WELL-KNOWN ADMIN PSW.

10% CHECKED FOR BUGS IN WEB APPLICATIONS THE SERVERS MIGHT HAVE BEEN RUNNING

29% TRIED TO GET AT USER ACCOUNTS USING BRUTE FORCE TECHNIQUES THAT TRIED COMMONLY USED PASSWORDS

7% SOUGHT LOOPHOLES IN THE OPERATING SYSTEM SOFTWARE THE SERVERS WERE SUPPOSEDLY RUNNING
THE STOLEN IDENTITIES ARE USED FOR DIFFERENT PURPOSES:

- ACCESS TO CONFIDENTIAL DATA
- STEELING MONEY THROUGH EG. CEO FRAUD
- APPLY FOR LOANES TO BY INSURANCES, BUY PHONE SUBSCRIPTIONS
- ONLINE SERVICES, GAMES ETC.
- SOLD ON THE DARK WEB

IDENTITY THEFT HAS GROWN TO MORE THAN 89,000 REPORTED CASES IN GB IN THE FIRST HALF 2017.

3.1 BILLION RECORDS WERE LEAKED IN 2016
THE EMERGING LANDSCAPE OF CYBERTHREATS

YOUR ORG & STAFF

INADVERTENT DATA LEAKS (EMAIL & WEB) SOCIAL ACCOUNTS

ACTIVE

NETWORK & APPLICATION HACKING

DATA HARVESTED & SOLD ON DARK WEB

DATA HARVESTING

TIME FRAME FROM HARVESTING TO ATTACK COULD BE UP TO 2 YEARS

YOUR ORG OR STAFF

TARGETED ATTACK

DARK WEB

RANSOMWARE-AS-A-SERVICE MODELS, ENSURES THAT ANY “WOULD-BE CRIMINAL” CAN UTILIZE THE RANSOMWARE SOFTWARE, REGARDLESS OF THEIR TECHNICAL KNOWLEDGE.

50% OF ALL COMPANIES SUFFERED FROM RANSOMWARE AND NOT ALL FULLY RECOVERED.

THE LATEST TYPES OF RANSOMWARE, COMPEEDS WITH GDPR AND THREATENS TO PUBLISH YOUR DATA IF YOU DON’T PAY THE RANSOM.
IN AUGUST 2017 HBO ASSUMINGLY WERE EXPOSED TO HACKING AND CLAIMS OF RANSOM CRIMINALS THREATNED TO PUBLISH HBO'S ACCOUNTS, NEW SECTIONS OF GAME OF THRONES AND BRAND NEW SERIES COMMING UP.

NO PROOF OF ACTUAL HACKING WAS PROVIDED. HBO'S COMMENTS INDICATES THE SAME.

THIS COULD BE WHALING OR INSIDERS THAT MIGHT HAVE VOLUNTEERED TO LEAK THE INFORMATION.
THE SOURCE COULD BE NON LOYAL EMPLOYEES OR DISSATISFIED / OPPORTUNISTIC FORMER EMPLOYEES, PERHAPS COMBINED WITH COLLABORATION WITH EXTERNAL IT CRIMINALS.

LESSON LEARNED: THE IMPORTANCE OF SEPARATION OF SYSTEMS, ACCESS AND DUTIES. A GOOD COMPANY CULTURE IS VERY IMPORTANT.
YOSEE
JUNE 11TH 2017 YOUSEE CUSTOMERS WERE ABLE TO ACCESS AND CHANGE EACH OTHERS SUBSCRIPTION AGREEMENTS, BILLS AND ORDER NEW SIM CARDS ON BEHALF OF OTHER USERS IN THE YOUSEE’S SELF SERVICE PORTAL.

YOUSEE WAS CRITIZED FOR TAKING SEVERAL HOURS TO CLOSE THE ACCESS DOWN

INCOMPLETE PROGRAMMING AND/OR CONFIGURATION IS AN INCREASING PROBLEM FOR MANY COMPANIES. THE TIME TO MITIGATE IS ANOTHER BIG PROBLEM....... 

LESSON: DO THOUROUGH CHECKS ON PROGRAMMING AND UPDATES AND MAKE SWIFT RECOVERY AND ACTION PLANS
CSC/ DANISH POLICE
THE FAMOUS HACK AGAINST CSC/ DANISH POLICE PROVIDED ACCESS TO DATA TO AND FROM THE DANISH CPR-REGISTER, THE REGISTER FOR DRIVERSLICENSES AND THE SCHENGEN INFORMATIONS SYSTEM WITH INFORMATION ON WANTED EUROPEANS.

• A ZERO DAY VULNERABILITY WAS USED TOGETHER WITH LOCAL ADMIN RIGHTS
• AN OPEN WEBSERVER WITH REGISTERED PENSION DATA WAS RUNNING ON THE SAME SERVER
• THE DANISH GOVERNMENT IT REVISIONS RECOMMENDATIONS FOR PATCHING 5 MONTHS EARLIER WAS NOT FOLLOWED.

IMPLICATIONS: THE HACKER PER GOTTFRID SVARTHOLM WARG WERE CENTENSED AND MANY DANISH CITIZENS DATA WERE COMPROMISED. NO ONE KNOWS – THE FINAL SCOPE OF IMPLICATIONS.

LESSON: ENSURE PATCHING, SEGMENTATION, LOGGING AND NO LOCAL ADMIN RIGHTS
IBM AND THE SWEDISH TRANSPORT AGENCY

IBM PROCESSED DATA FOR THE SWEDISH TRANSPORT AGENCY, WHICH INCLUDED SWEDISH AGENTS' IDENTITIES, POLICE OFFICERS, MILITARY AND SECURITY AGENTS ETC. TO KEEP COSTS DOWN, THE RULES IN THE AGREEMENT DID NOT STIPULATE THAT DATA MUST REMAIN IN THE COUNTRY AND THAT THEY MAY ONLY BE PROCESSED BY SECURITY-APPROVED SWEDISH EMPLOYEES.

WHEN REVEALED AND BEFORE THE POLICE REPORT WAS FINALIZED, THE GENERAL SECRETARY OF THE TRANSPORT AGENCY WAS FIRED AND SUBSEQUENTLY SHE WAS SENTENCED FOR CARELESS HANDLING OF CONFIDENTIAL INFORMATION AND BREACH OF THE PRIVACY DATA PROTECTION RULES. THE FINE WAS 70,000 SEK.

LESSON: SECURE SOURCING MUST BE SELECTED AND DOCUMENTED WITH CERTAINTY AND APPLICABLE LAW IN MIND.
EXAMPLE

WANNACRY
IN MAY 2017 WANNACRY- A LARGE CYBER-ATTACK WAS LAUNCHED IN 28 DIFFERENT LANGUAGES. CLAIMING RANSOM PAYMENT IN BITCOINS

A VULNERABILITY (PATCHED 2 MONTHS BEFORE) IN THE SMB PROTOCOL IN WINDOWS, MADE IT POSSIBLE FOR THE MALWARE TO AUTOMATICALLY COPY ITSELF TO OTHER AVAILABLE NETWORK TARGETS. CONSEQUENTLY INFECTING MORE THAN 230,000 COMPUTERS IN 99 COUNTRIES

LESSON:
HAVE AN UPDATED AND SOUND FIREWALL POLICY, BETTER PROGRAMMING AND EFFICIENT PATCHING CAN PREVENT THESE TYPES OF ATTACKS
NOTPETYA
TARGETING PRIMARELY UKRAINE, BUT ALSO REACHED MÆRSK AND SEEMS TO HAVE BEEN CRAFTED BY A FOREIGN STATE EG. RUSSIA

THE METHOD USED INDICATES THAT NOTPETYA WAS NOT INTENDED AS RANSOMWARE BUT RATHER
A DATA DESTRUCTION TOOL IN DISGUISE THAT COULD STEAL DATA AND PASSWORDS. SOURCE OF THE INFECTION COULD BE EG. AN UPDATE SERVER FOR ACCOUNTING SOFTWARE

LESSON: PATCHING PATCHING PATCHING....
INCREASED SPEARPHISHING, INDUSTRIAL ESPIONAGE, CYBER ATTACKS DIRECTLY AT, - OR THROUGH SUB-CONTRACTORS TO CRITICAL INFRASTRUCTURE.

GATEWAY SECURITY, SECURE DNS, ENDPOINT SECURITY ETC. WILL HELP PROTECT YOUR SYSTEMS, BUT UP TO 10,5% OF THE THREATS WILL BE UP TO END USERS TO PREVENT.
FINALLY WE GET SOME REGULATIONS EG. GDPR THAT REQUIRES:

- ACCOUNTABILITY, RESPONSIBILITY, INTEGRITY, CONTROL AND DOCUMENTATION OF DATAFLOWS, SYSTEMS, AGREEMENTS AND DATAHANDLING
- PRIVACY BY DEFAULT AND BY DESIGN
- TRANSPARENCY TOWARDS THE REGISTERED PERSONS AND CONCENT
- DATAMINIMIZATION
- DATA PRIVACY IMPACT ASSESSMENTS
- AND INFORMATION TO THE DATA AGENCY IN CASE OF DATA BREACH
• WHAT DATA DO YOU HAVE AND HOW DOES IT FLOW?

• WHO HAS ACCESS TO YOUR DATA AND HOW?

• A DATA MINIMIZATION PROJECT IN CONNECTION WITH CLARIFICATION OF DATA FLOWS, NOT ONLY REDUCES THE BURDEN OF GDPR, BUT CAN ALSO PROVIDE SAVINGS BY CHANGED AND SIMPLIFIED WORKFLOWS WHEREVER POSSIBLE.

• CLOUD AND HOSTING AGREEMENTS - ARE THEY SAFE AND DO THEY COMPLY TO GDPR?
NOW THAT YOU HEARD ABOUT THE THREATS YOU PROBABLY REALIZE THE UPSIDE OF

A SECURITY IMPACT AND RISK ASSESSMENT.
SECURITY CHECK

• BACK UP, - IF- THEN HOW FAST CAN YOU GET UP RUNNING AGAIN?

• CHECK TECNOLOGIES IN USE AND HOW THEY ARE CONFIGURED.

• TECHNOLOGIES MISSING (ENCRYPTION, PSEUDONYMISATION, AUTHENTIFICATION, PATCH MANAGEMENT, SECURE DNS, APT, SECURE FILESHARING ETC.)
• NO LOKAL ADMINISTRATOR RIGHTS

• PASSWORD POLITICS- ENSURE COMPLIANCE

• SEPARATION OF DUTIES AND SYSTEMS

• MULTI FAKTOR AUTHENTIFICATION, TO ENSURE RIGHT ID ACCESS AND TO SUPPORT SEPARATION OF DUTIES AND SYSTEMS.

• PRIVILEGED ACCESS MANAGEMENT AND IDENTITY MANAGEMENT, FOR CONTROLLING SYSTEM-LEVEL PRIVILEGES, ACCESS, AND IDENTITIES

• DIGITAL SIGNATUR. FOR CONCENTS AND BINDING AGREEMENTS AS WELL AS FOR VERIFICATION OF VALIDITY OF THE WEBSITES IDENTITY AND/OR FOR ENCRYPTING DATA
TECHNICAL MEASURES

• ENDPOINT SECURITY:
  • PASSWORD MANAGEMENT
  • ANTIMALWARE
  • CLIENT BASED FIREWALL (IDS OG IPS)
  • BROWSER SECURITY
  • APPLIKATION SECURITY
  • AUTHENTIFICATION
  • PATCHING
  • REGISTRATION OF SYSTEM CHANGES
  • ENCRYPTION OF FILES, DISKS AND DEVICES
• **PATCH MANAGEMENT** ON NETWORK LEVEL

• **NEXT GENERATION FIREWALLS** – **WITH** INTRUSION PREVENTION SYSTEM AND ADVANCED PERSISTENT THREAT.

• **WEBFILTERING**

• **SECURE DNS**

• **DATA LEAKAGE PREVENTION** (EG. CONTENTFILTERING AND ENCRYPTION IN WEB-, MAILSYSTEMS AND FIREWALLS)
TECHNICAL MEASURES

• SECURE FILESHARING - WHO ARE HOLDING THE KEYS?

• SHADOW IT DISCOVERY – WHATS ON YOUR NETWORK?

• LOG AND NETWORK MONITORING – WHAT HAPPENS ON THE NETWORK?
PREVENT THIRD PARTY INSIGHT

IT CAN BE SOLVED WITH:

• ENCRYPTION OF DATA, DISKS, MEDIAS, FILES, FOLDERS, COMMUNICATION, ACCESS.

• OBFUSCATING DATA

• ANONYMISING DATA

“For security purposes, the information should make no sense at all to spies and hackers. We’ll bring in someone later to figure out what you meant.”
SECURE DATA DESTRUCTION AND DATA REDACTION
THINK PRIVACY BY DESIGN AND BY DEFAULT INTO ALL PROCEDURES, PRODUCTS AND STRATEGIES
RECOMMANDATIONS

MAKE A REALISTIC DISASTER RECOVERY PLAN

SELECT FORENSIC SPECIALISTS BEFORE YOU NEED THEM. THEY WILL BE ABLE TO SECURE DATA AND FOLLOW "CHAIN OF CUSTODY" FOR THE FURTHER USE AT CORT.
WORK ON SECURITY AWARENESS;
TEST KNOWLEDGE ABOUT IT SECURITY, IT POLITICIES AND PROCESSES ON ALL LEVELS IN THE COMPANY AND PREFERABLY ALSO TEST IMPORTANT ASSOCIATES.

EG. MAKE
• QUESTIONNAIRES
• SIMULATED PHISHING ATTACKS
• ”TAILGATING”
• ”PLANTING” OF E.G. USB KEYS OR RASPBERRY PI’S
• SOCIAL ENGINEERING – CHOCOLATE OR WINE IN CHANGE FOR INFORMATION
THE REAL INCENTIVE

THE COMPANY IS THE FUTURE OF THE EMPLOYEES ........................................
.................................................................................................................AND THEY ARE THE FUTURE OF THE COMPANY

• WORK WITH THE GENERAL CULTURE AT YOUR ORGANIZATION AND LOYALTY TOWARDS COLLEAGUES AND THE COMPANY

• LET THE EMPLOYEES TAKE RESPONSIBILITY
RECOMMANDATIONS

ORGANIZE FYSICAL ACCESS CONTROLS FOR AUTHORISED ACCESS ONLY
IT IS NOT ONLY FOR WHAT WE DO THAT WE ARE HELD RESPONSIBLE, BUT ALSO FOR WHAT WE DO NOT DO

/Moliere
ISO 2700X

- INCIDENT RESPONSE
- RISK MANAGEMENT
- RISK ASSESSMENT
- SECURITY ASSESSMENT
- GDPR COMPLIANCE
- SECURITY AWARENESS TRAINING

- SUPPORT
- NETWORK SECURITY
- INFORMATION SECURITY POLICIES
- SECURITY BASELINE
- PHYSICAL SECURITY TEST
- PROJECT MANAGEMENT (SCRUM OR PRINCE2 BASED)
VULNERABILITY MANAGEMENT
ANTIVIRUS

PENETRATION TEST
PATCHING

VULNERABILITY TEST
ENCRYPTION

LOAD BALANCING
MDM

DDoS PREVENTION
BACK-UP

LOG MANAGEMENT
MAIL FILTERING

NETVÆRK MONITORING
AUTHENTIFICERING

SECURE DNS
FIREWALL

PRIVELEGED ACCESS CONTROL
INTRUSION PREVENTION

WEB FILTERING
C-CURE HELPS TO TIMELY COMPLIANCE TO GDPR

WE CAN EITHER PERFORM THE PRIMARY WORK FOR YOU, ACT AS YOUR DPO, OR JUST HELP WITH THE PREPARATION OF DOCUMENTATION ....

AND THE INVOLVEMENT OF THE NECESSARY INTERNAL AND EXTERNAL PARTIES ON; TECHNOLOGIES, RISK ASSESSMENT, DATA RESPONSIBILITY, COMPUTING, LAW, HR, AUDIT, ETC.

REMEMBER:
SELECT ADVICE FROM BOTH LAWYERS AND TECHNICAL KNOWLEDGEABLE ADVISERS
USE ISO27002 AS CONTROLS TO MAKE SURE YOU COMPLY TO YOUR OWN GOALS AND LAWS.

C-CURE HAS MADE GDPR TEMPLATE IN DANISH, THAT IS FREE FOR DOWNLOAD. YOU WILL FIND IT ON OUR WEBPAGE (IN DANISH)
C-CURE
DRONNINGGÅRDS ALLE 138
DK 2840 HOLTE
DENMARK
TLF. 45411446

CEO: METTE NIKANDER
MAIL: MN@C-CURE.DK
SUPPORT: SUPPORT@C-CURE.DK