ondeso
The Industrial IT Company.

Water-holing, Spear-phishing & Back Doors

ondeso GmbH - April 2019

Water-holing (watering hole attack)

Beschreibung

„Water-holing“ ist das Auflauern an einer vertrauenswürdigen Quelle und „Vergiften“.

Gerichteter Angriff auf eine spezielle Personengruppe.

Szenarien

- Angriff auf Webseite oder FTP-Server eines Softwareherstellers
- Signatur mit offengelegten Zertifikaten

Water-holing - Beispiele

The Hacker News https://thehackernews.com/

Heise Security
https://heise.de/security/

Water-holing

Risiken

Blindes Vertrauen in die Quelle oder Signaturen

Technische Maßnahmen

- Prüfsummen (aus anderer Quelle!)
- Schwachstellen durch Softwareupdates minimieren
- Sandboxing

Organisatorische Maßnahmen

- Zentrale Prüfung und Bereitstellung von Software, Konfigurationen,…
- Vier-Augen-Prinzip bei Sichtung von Geräten und Software
- Datenaustausch über geschützte Portale

Water-holing

Risiken

Blindes Vertrauen in die Quelle oder Signaturen

T

…isatorische Maßnahmen

AWARENESS SCHAFFEN

- Prüfsummen (aus anderer Quelle!)
- Schwachstellen durch Softwareupdates minimieren
- Sandboxing

- Zentrale Prüfung und Bereitstellung von Software, Konfigurationen,…
- Vier-Augen-Prinzip bei Sichtung von Geräten und Software
- Datenaustausch über geschützte Portale

Spear-phising

Beschreibung

„Spear-phishing“ der gezielte, gut vorbereitete und vermeintlich vertrauenswürdige Email-Angriff auf einen speziellen Personenkreis oder einzelne Personen.

Dynamite Phishing automatisiertes Spear-phising

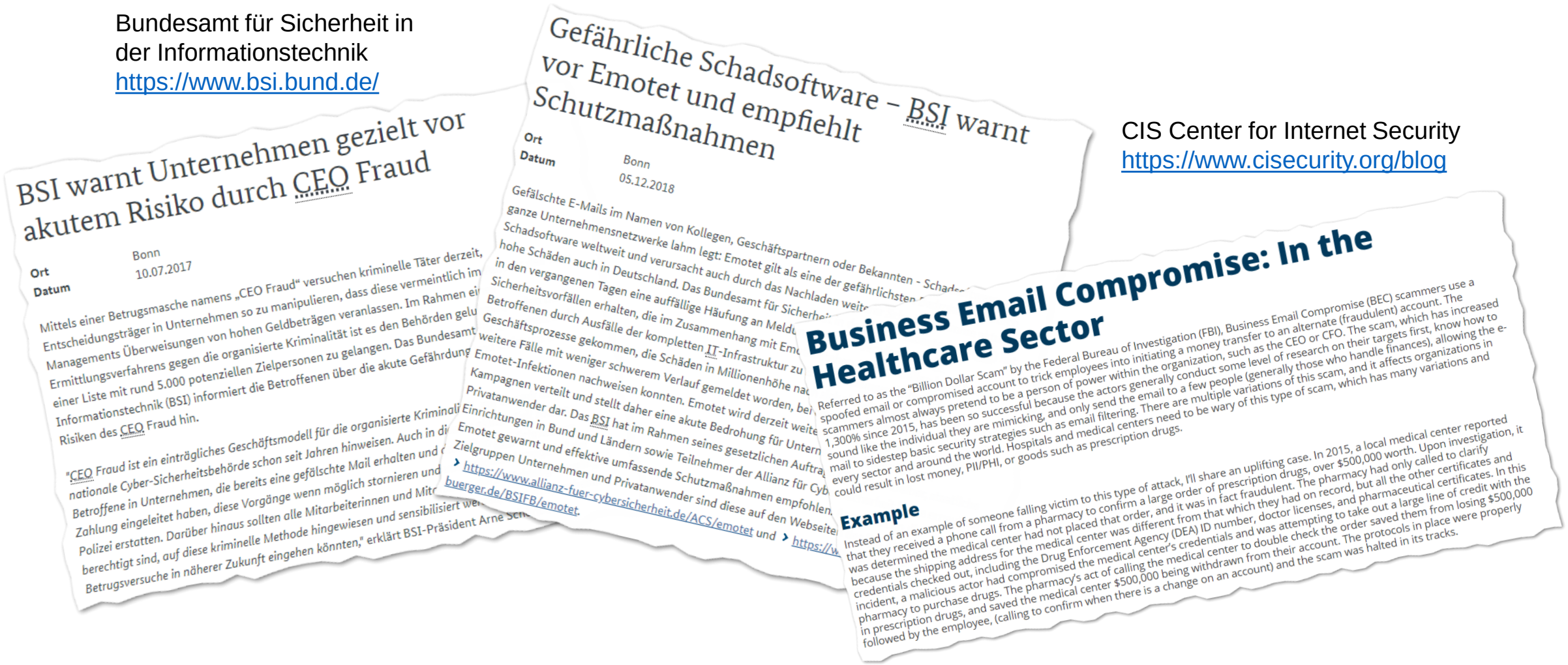
Whaling / BEC (Business Email Compromise)

Szenarien

- Bewerbungsunterlagen an HR (Emotet)
- Transaktionsanweisungen vom CEO an Finanzabteilungen (CEO Fraud)
- Projektupdate an Anlagenbetreiber

Spear-phising - Beispiele

Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de/



BSI warnt Unternehmen gezielt vor akutem Risiko durch CEO Fraud

Ort Bonn
Datum 10.07.2017

Mittels einer Betrugsmasche namens „CEO Fraud“ versuchen kriminelle Täter derzeit, Entscheidungsträger in Unternehmen so zu manipulieren, dass diese vermeintlich im Managements Überweisungen von hohen Geldbeträgen veranlassen. Im Rahmen ei Ermittlungsverfahrens gegen die organisierte Kriminalität ist es den Behörden gelu einer Liste mit rund 5.000 potenziellen Zielpersonen zu gelangen. Das Bundesamt Informationstechnik (BSI) informiert die Betroffenen über die akute Gefährdung Risiken des CEO Fraud hin.

"CEO Fraud ist ein einträgliches Geschäftsmodell für die organisierte Kriminali nationale Cyber-Sicherheitsbehörde schon seit Jahren hinweisen. Auch in di Betroffene in Unternehmen, die bereits eine gefälschte Mail erhalten und Zahlung eingeleitet haben, diese Vorgänge wenn möglich stornieren und Polizei erstatten. Darüber hinaus sollten alle Mitarbeiterinnen und Mitarbeiter berechtigt sind, auf diese kriminelle Methode hingewiesen und sensibilisiert Betrugsversuche in näherer Zukunft eingehen könnten," erklärt BSI-Präsident Arne Schönbohm.

Gefährliche Schadsoftware – BSI warnt vor Emotet und empfiehlt Schutzmaßnahmen

Ort Bonn
Datum 05.12.2018

Gefälschte E-Mails im Namen von Kollegen, Geschäftspartnern oder Bekannten - Schadsoftware, die ganze Unternehmensnetzwerke lahm legt: Emotet gilt als eine der gefährlichsten Schadsoftware weltweit und verursacht auch durch das Nachladen weiterer Schadsoftware hohe Schäden auch in Deutschland. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in den vergangenen Tagen eine auffällige Häufung an Meldungen zu Emotet-Infektionen und Sicherheitsvorfällen erhalten, die im Zusammenhang mit Emotet stehen. Betroffenen durch Ausfälle der kompletten IT-Infrastruktur zu Geschäftsprozesse gekommen, die Schäden in Millionenhöhe nach sich ziehen. weitere Fälle mit weniger schwerem Verlauf gemeldet worden, bei denen Emotet-Infektionen nachweisen konnten. Emotet wird derzeit weiterentwickelt und Kampagnen verteilt und stellt daher eine akute Bedrohung für Unternehmen, Privatanwender dar. Das BSI hat im Rahmen seines gesetzlichen Auftrags Einrichtungen in Bund und Ländern sowie Teilnehmer der Allianz für Cybersicherheit Emotet gewarnt und effektive umfassende Schutzmaßnahmen empfohlen. Zielgruppen Unternehmen und Privatanwender sind diese auf den Webseiten

› https://www.allianz-fuer-cybersicherheit.de/ACS/emotet und › https://www.bsi-fuer-buerger.de/BSIFB/emotet.

Business Email Compromise: In the Healthcare Sector

Referred to as the “Billion Dollar Scam” by the Federal Bureau of Investigation (FBI), Business Email Compromise (BEC) scammers use a spoofed email or compromised account to trick employees into initiating a money transfer to an alternate (fraudulent) account. The scammers almost always pretend to be a person of power within the organization, such as the CEO or CFO. The scam, which has increased 1,300% since 2015, has been so successful because the actors generally conduct some level of research on their targets first, know how to sound like the individual they are mimicking, and only send the email to a few people (generally those who handle finances), allowing the e-mail to sidestep basic security strategies such as email filtering. There are multiple variations of this scam, and it affects organizations in every sector and around the world. Hospitals and medical centers need to be wary of this type of scam, which has many variations and could result in lost money, PII/PHI, or goods such as prescription drugs.

Example

Instead of an example of someone falling victim to this type of attack, I'll share an uplifting case. In 2015, a local medical center reported that they received a phone call from a pharmacy to confirm a large order of prescription drugs, over $500,000 worth. Upon investigation, it was determined the medical center had not placed that order, and it was in fact fraudulent. The pharmacy had only called to clarify because the shipping address for the medical center was different from that which they had on record, but all the other certificates and credentials checked out, including the Drug Enforcement Agency (DEA) ID number, doctor licenses, and pharmaceutical certificates. In this incident, a malicious actor had compromised the medical center's credentials and was attempting to take out a large line of credit with the pharmacy to purchase drugs. The pharmacy's act of calling the medical center to double check the order saved them from losing $500,000 in prescription drugs, and saved the medical center $500,000 being withdrawn from their account. The protocols in place were properly followed by the employee, (calling to confirm when there is a change on an account) and the scam was halted in its tracks.

CIS Center for Internet Security
https://www.cisecurity.org/blog

Spear-phising

Risiken

Glaubwürdigkeit des Absenders

Evtl. wird Druck durch einen vermeintlichen Vorgesetzten erzeugt

Technische Maßnahmen

- Mailfilter: z.B. Abgleich der Anzeigenamen mit Antwortadressen
- Patchen bzw. Updaten der Software
- Mail an bekannte Adresse (nicht einfach antworten - UTF-8 Domains!)

Organisatorische Maßnahmen

- Zusätzliche Prüfungsmechanismen z.B. Rückruf per Telefon
- Keine Mails von unbekannten/unerwarteten Kontakten öffnen
- VORSICHT bei Anhängen!

Spear-phising

Risiken

Glaubwürdigkeit des Absenders

Evtl. wird Druck durch einen vermeintlichen Vorgesetzten erzeugt

Maßnahmen

- Mailfilter: z.B. Abgleich der Anzeigenamen mit Antwortadressen
- Patchen bzw. Updaten der Software
- Mail an bekannte Adresse (nicht einfach antworten - UTF-8 Domains!)

- Zusätzliche Prüfungsmechanismen z.B. Rückruf per Telefon
- Keine Mails von unbekannten/unerwarteten Kontakten öffnen
- VORSICHT bei Anhängen!

Back Doors

Beschreibung

Back Doors sind nicht offen kommunizierte Zugriffsmöglichkeiten
z.B. des Herstellers (für den Notfall)

Szenarien

- Default Passwörter
- Einschränkung durch Folientastatur z.B. nur Zahlen und Großbuchstaben
- Passwörter zur Verbindung innerhalb des Systems im Klartext z.B. in der Registry oder in Skripten
- NOBUS – Nobody But US

Back Doors - Beispiele

Heise Security
https://heise.de/security/

Tom‘s HARDWARE
https://www.tomshardware.com/t/security/

13.01.2018 12:19 Uhr

Lenovo findet Backdoor in eigenen Netzwerk-Switches

Die kompromitierten Switch-Modelle, die nun zu Lenovos Portfolio g
hatte ursprünglich der längst aufgelöste Netzwerk-Zulieferer Norte

Von Dusan Zivadinovic

Die Geschichte von Junipers enteigneter Hintertür

Lesetipp 07.08.2017 15:13 Uhr – Monika Ermert

(Bild: Juniper)

In einem mehrfach ausgezeichneten Paper liefern Forscher eine Art Krypto-Krimi. Sie dokumentieren minutiös, wie der Netzwerkausrüster Juniper eine versteckte Hintertür in seine Produkte einbaute – und wie ein externer Angreifer sie später umfunktionierte.

URITY > NEWS

ackdoors Keep Appearing In Cisco's Routers

10 COMMENTS

by Lucian Armasu July 19, 2018 at 10:00 AM - Source: Cisco Tools

Over the past few months, not one, not two, but five different backdoors joined the list of security flaws in Cisco routers.

Cisco Architecture for Lawful Intercept

Way back in 2004, Cisco wrote an IETF proposal for a "lawful intercept" backdoor for routers, which law enforcement could use to remotely log in to routers. Years later, in 2010, an IBM security researcher showed how this protocol could be abused by malicious attackers to take over Cisco IOS routers, which are typically sold to ISPs and other large enterprises.

Back Doors - Beispiele

ZDNet
https://www.zdnet.de/

13.01.2018 12:19 Uhr

Lenovo findet Backdoor in eigenen Netzwerk-Switches

Die kompromitierten Switch-Modelle, die nun zu Lenovos Po
hatte ursprünglich der längst aufgelöste Netzwerk-Zuliefere

Von Dusan Zivadinovic

ZDNet / Sicherheit / Authentifizierung

Studie: Programmierer schlampen bei der Passwortsicherheit

Forscher geben ein Registrierungssystem für Nutzer eines Sozialen Netzwerks in Auftrag. 18 von 43 freiberuflichen Entwicklern speichern die Kennwörter dabei im Klartext. Insgesamt setzen nur 17 auf als sicher geltende Verschlüsselungsverfahren.

von Stefan Beiersmann am 11. März 2019 , 10:47 Uhr

Eine Studie (PDF) des Instituts für Informatik 4 der Universität Bonn hat ergeben, dass freiberufliche Programmierer von sich aus nicht immer Regeln für das sichere Speichern von Passwörtern befolgen. Bei einem Test mit 43 Entwicklern gingen viele den einfachen Weg und speicherten Kennwörter ohne eine ausreichenden Schutz vor Diebstahl und unberechtigten Zugriffen.

10 COMMENTS

Back Doors

Risiken

Wird aus Bequemlichkeit und für Notfälle geduldet

Ist pragmatisch („praktisch“)

Technische Maßnahmen

- 2-Factor Authentisierung ggf. über Token
- Passwortänderung bei automatisierter Installation oder Inbetriebnahmeprozess berücksichtigen

Organisatorische Maßnahmen

- Anforderung bei der Planung
- Prüfen von Onlineforen oder Dokumentation
- Dokumentieren und melden

Back Doors

Risiken

Wird aus Bequemlichkeit und für Notfälle geduldet

Ist pragmatisch („praktisch“)

Tec

Bnahmen

AWARENESS SCHAFFEN

- 2-Factor Authentisierung ggf. über Token
- Passwortänderung bei automatisierter Installation oder Inbetriebnahmeprozess berücksichtigen

- Anforderung bei der Planung
- Prüfen von Onlineforen oder Dokumentation
- Dokumentieren und melden

Zusammenfassung

Ist Ihre Organisation darauf vorbereitet, dass z.B. Images oder Software Ihres Leitsystemherstellers (ohne dessen Wissen) manipuliert wurden?

Oder verlassen Sie sich auf die Kontrolle Ihrer Hersteller und Lieferanten?

Sind Ihre Mitarbeiter darauf geschult, gezielte Fehlinformationen zu erkennen?

Oder verlassen Sie sich auf SPAM-Filter und Virenscanner?

Kennen Sie oder einer Ihrer Mitarbeiter Default oder Universal-Passwörter?

Was hätte es für Auswirkungen, wenn diese auch anderen Personen außerhalb Ihrer Organisation bekannt wären?

Fazit

Das eigene Unternehmen schützen vor:

Ziel eines Angriffs

Quelle für Weiterverbreitung

1. Berücksichtigung des ganzen Lifecycles bereits bei der Planung neuer Anlagen
   - Vorgaben für Updatezyklen, Verträglichkeit, Freigaben,…
   - Detaillierte Dokumentation des Auslieferungszustandes
2. Informationen über den Zustand der eigenen Infrastruktur müssen jederzeit abrufbar sein!
3. Updaten der Software und bekannte Schwachstellen schließen
4. Backups für Desaster Recovery oder vollständig automatisierte Installationsprozesse
5. Kennwörter/User kurzfristig ändern können (auch ohne ActiveDirectory!)
6. Prozesse und deren Schnittstellen (physisch/virtuell) absichern
7. …

Quellen / weiterführende Links

- **Bundesamt für Sicherheit in der Informationstechnik (BSI)**
  Cyber-Sicherheit in Industrieanlagen und -steuerungen
  https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/ICS/ics_node.html

  IT-Grundschutz – IND: Industrielle IT
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_Uebersicht_node.html
- **if(is) internet-sicherheit.**
  Institut für Internet-Sicherheit für mehr Vertrauenswürdigkeit und IT-Sicherheit
  https://www.internet-sicherheit.de/
- **SANS Technology Institute**
  Cyber Security Research
  https://www.sans.edu/cyber-research
- **Heise online**
  heise Security
  https://www.heise.de/security/

ondeso
The Industrial IT Company.

Vielen Dank für Ihre Aufmerksamkeit.

☛ Halle 6, Stand E07

ondeso GmbH
Peter Lukesch, COO
Blumenstraße 16a · 93055 Regensburg · Germany · www.ondeso.com
Phone: +49 941 462932-0 · Fax: +49 941 462932-99 · E-Mail: info@ondeso.com