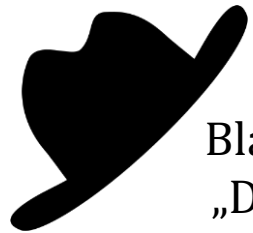




Kriminelle und Praxen -Angreiferperspektive-

Wer sind die Angreifer?

Moral
IT-Sicherheitsspezialisten



Blackhats
„Die Bösen“

- Brechen in Systeme ein
- Brechen Gesetze



Um die geht es heute



Greyhats
„Die Antihelden“

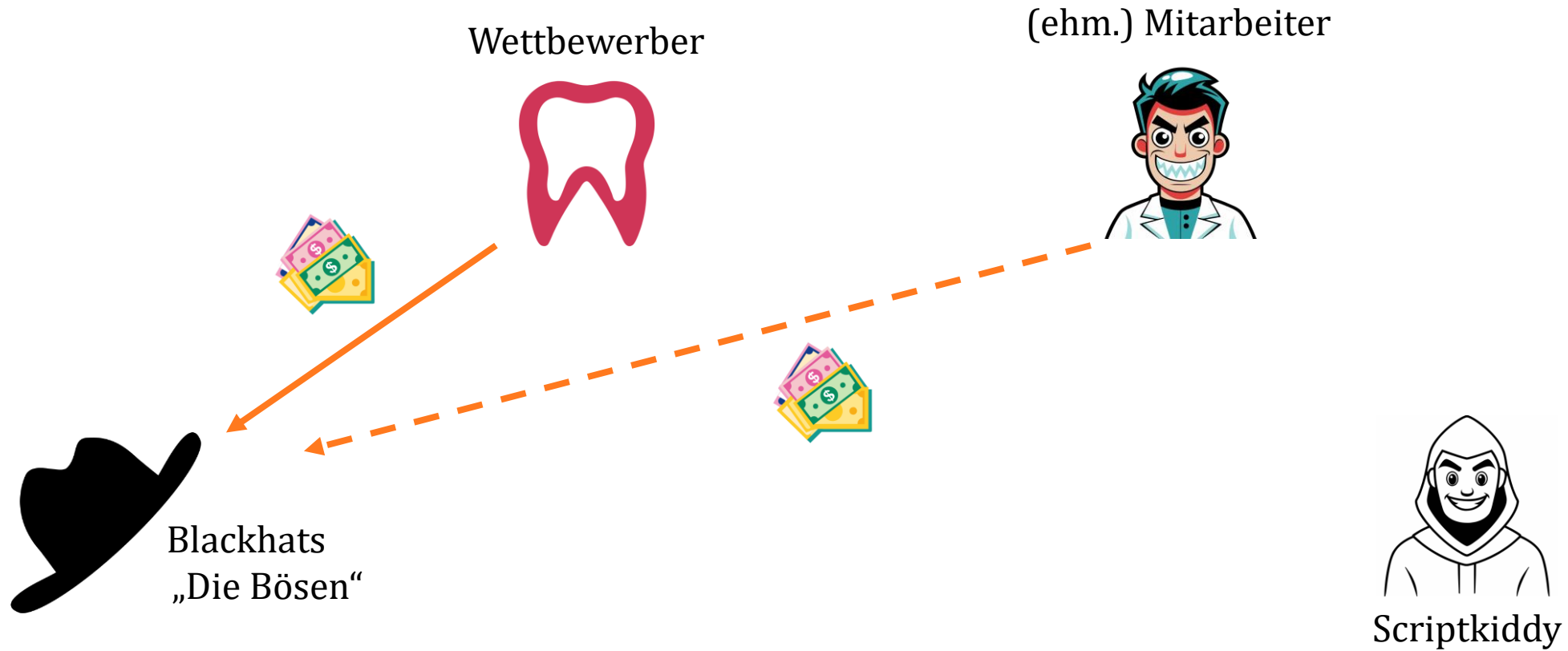
- Sichern Systeme ab
- Halten sich nicht immer an Gesetze



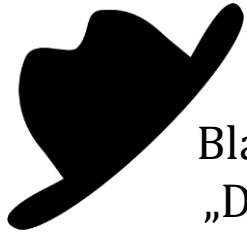
Whitehats
„Die Guten“

- Sichern Systeme ab
- Gesetzestreu

Wer sind die Angreifer?



Warum? Motivation / Ziel der Angreifer



Blackhats
„Die Bösen“

- Geld
- Spionage

Wettbewerber



- Geld
- Spionage
- Wettbewerbs-
behinderung

(ehm.) Mitarbeiter



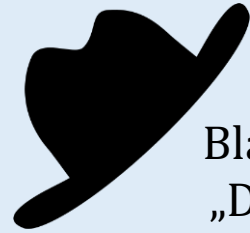
- Rache
- Geld

Scriptkiddy



- Neugier
- Zerstörungs-
wille

Wir sind...



Blackhats
„Die Bösen“

Für den weiteren Verlauf sind wir
„Blackhats“



Warum Zahnärzte?



Pro

- Ärzte gelten als „Gutverdiener“
- Wertvolles Equipment
- Wertvolle Daten
- Zugang zu reglementierten Substanzen
- Bekannte Adressen + Öffnungszeiten
- Niederschwelliger Zugang zu Räumlichkeiten („Patientenstrom“)

Contra

- Aufgrund rechtlicher Vorschriften erhöhtes Schutzniveau (TI, KRITIS, ...)

Wie kann ich Geld „verdienen“?



- Klassiker
 - Auftrag (Wettbewerber, Mitarbeiter, ...)
 - Einbruch + Diebstahl von Geräten (und Daten)
 - Versendung gefälschter Nachrichten (Post) / Zahlungsaufforderung
 - Installation von Schadsoftware
 - Stehlen von Zugangsdaten zum Onlinebanking
 - Daten verschlüsseln / Erpressen (Ransomware)
 - Daten stehlen + Verkaufen
 - Social Engineering / Anruf: drängen zum Überweisen von Betrag X



Angriffsvektoren – Einbruch / Diebstahl



- Geld verdienen durch Verkauf von Diebesgut
 - Hohes Risiko, da Präsenz zwingend erforderlich
 - Nur bestimmtes Diebesgut einfach „veräußerbar“
 - Es kann nicht alles abtransportiert werden (Gewicht + Zeitfaktor vs. Risiko)
- Nur Dinge stehlen, die „leicht“ sind, und einen hohen Wert haben
- Laptops, Tablets, Smartphones, Externe Festplatten, Medikamente



Angriffsvektoren – Einbruch / Diebstahl



- Nach dem Diebstahl
 - Prüfen der Geräte auf wertvolle Daten, z.B. Zugangsdaten, Patientendaten, ...
- Wird schnell bemerkt

**Diebstahl von IT-Geräten ist ggf. ein meldepflichtiger Sicherheitsvorfall
(BSI-KRITIS Verordnung, NIS2, ...)**



Angriffsvektoren – Phishing



- Ziel: Diebstahl von Zugangsdaten oder Zahlungsdaten
 - Onlinebanking
 - E-Mail Postfächer
 - Kreditkarten
- Geld verdienen durch:
 - Leerräumen der Konten
 - Belastung der Kreditkarte
 - Verkauf von Zugangsdaten
 - Verkauf von Infos aus Postfächern

Angriffsvektoren - Phishing



Antworten Allen antworten Weiterleiten



Do 28.07.2022 07:53

Re: Beratungsstelle

An

Links und sonstige Funktionen wurden in dieser Nachricht deaktiviert. Verschieben Sie die Nachricht in den Posteingang, um diese Funktionen zu aktivieren.
Diese Nachricht wurde in das Nur-Text-Format konvertiert.

Angestellte/Mitarbeiter.

Heute, am 28. Juli 2022, migrieren wir das gesamte E-Mail-Konto der Mitarbeiter und des Managements auf Outlook 2022 Office Webmail. Daher müssen alle Mitarbeiter und aktiven Mitarbeiter eine dringende Aktualisierung und Migration prüfen und sich dafür anmelden, um die Sicherheit und Effizienz aktueller Spam-E-Mails zu verbessern.

Alle Mitarbeiter und Führungskräfte müssen HIER KLICKEN <[https://\[REDACTED\]GWNn](https://[REDACTED]GWNn)> , um auf Outlook Webmail 2022 für Mitarbeiter und Mitarbeiter umzustellen.

Bitte beachten Sie, dass diese Migration zu Outlook 2022 für alle E-Mails dieses Dienstes gilt. Wir werden alle nicht aktivierten und inaktiven E-Mail-Konten, die nicht in den nächsten 24 Stunden migriert wurden, ohne Vorankündigung deaktivieren.

Kompliment,
Outlook-E-Mail-Administrator

Outlook-Dienst für Mitarbeiter und Internetdienst Copyright2022





Angriffsvektoren – Schadsoftware

- Ziel: Installation von Schadsoftware auf den Endgeräten
- Möglichkeiten Geld zu verdienen:
 - Daten kopieren + Verkaufen
 - Daten verschlüsseln + Erpressen (Ransomware)
 - Tastatureingaben mitlesen für Zugangsdaten (Keylogger)
 - Integration in ein Botnet + Vermietung
 - Vermietung / Verkauf des Zugangs zum Netzwerk
- Risiko geringer, da eine Präsenz nicht zwingend erforderlich ist





Angriffsvektoren – Schadsoftware

- Wie?
 - Gefälschte Mails mit gefährlichem Anhang / Link
 - Ausnutzen von Sicherheitslücken beim Surfen
 - „Liegen lassen“ von USB-Sticks mit böartigen Dateien
 - Social Engineering:
Sich als Techniker ausgeben, der eine Wartung durchführen muss
 - Via Telefon
 - Präsenz
- Kann lange unbemerkt bleiben



**Schadsoftware-Befall kann ein meldepflichtiger Sicherheitsvorfall sein
(BSI-KRITIS Verordnung, NIS2, ...)**

Wie kann ich sonst Geld „verdienen“?



- Spezialisiert auf Praxis
 - Social Engineering / Techniker:
Installation von bösartiger Hardware im Bereich „Kartenleser“ →
Medikamentenbeschaffung via E-Rezept
 - Blockierung der Internetleitung via DDoS
→ TI-Anbindung funktioniert nicht
→ Wettbewerbsbehinderung
- Via Patienten
 - Mittels gestohlener Daten formulierte Zahlungsaufforderungen
*„Bitte folgenden ausstehenden Betrag für die Behandlung am
11.12.2023 überweisen“*
 - Erpressung mittels gestohlener medizinischer Daten

Wie kann ich spionieren?



- Installation von Schadsoftware auf den Endgeräten
 - „Keylogger“ – Mitschnitt von Tastatureingaben
 - „Screencapture“ – Mitschnitt des Bildschirms
- Installation von böartiger Hardware im Netzwerk
- „Übernahme“ oder Installation von Überwachungskameras oder Webcams
- „Übernahme“ oder Installation von Mikrofonen



Zusammenfassung



- Zahnärzte = Lukratives Ziel für Angreifer
- Wer:
 - Blackhats, Wettbewerber, (ehm.) Mitarbeiter, Scriptkiddy
- Größte Motivation: Geld



Vielen Dank!

Für Fragen stehe ich Ihnen gern zur Verfügung.



Anhang

Wie kann ich „Rache“ nehmen?



- Verkauf von Wissen und Zugangsdaten
- Veröffentlichen von internen Infos (E-Mails, Verträge, Patientenstamm, ...)
- Zerstörung von Hardware / Vandalismus
- Zerstörung / Löschung von Daten

Wie? Angriffsvektoren



Digital



Präsenz

Wie? Angriffsvektoren



Digital

- Phishing
- DDoS (Distributed Denial of Service)
- Schadsoftware (Viren, Trojaner, ...)

Angriffsvektoren - Phishing

- Ziel
 - Abgreifen von Informationen
 - Ausführen von Handlungen, z.B. eine Überweisung auf ein Konto durchführen; eine Software installieren; ...
- Typische Merkmale von Phishing E-Mails
 - Es wird Druck aufgebaut, die zu einer sofortigen Handlung nötigen
 - Der Absender ist i.d.R. eine unbekannte E-Mail Adresse
 - Rechtschreib- und Grammatikfehler

Angriffsvektoren - DDoS

- Ziel
 - „Verstopfen“ der Internetleitung; Überfordern der Kapazität
 - Es ist kein oder nur noch eingeschränkter Netzzugang möglich
- Folge:
 - Internet nicht nutzbar → TI nicht nutzbar
 - „Verzögerungen im Betriebsablauf“ (Wettbewerbsbehinderung)
- Abhilfe
 - Mit dem eigenen Internet Service Provider über mögliche Maßnahmen sprechen (Telekom, Vodafone, 1und1, ...)

Angriffsvektoren - Schadsoftware

- Ziel(e)
 - Verschlüsselung von Daten
 - Datendiebstahl
 - Spionage
 - Datenzerstörung
- Abhilfe
 - Antivirensoftware
 - Awareness

Wie? Angriffsvektoren



Digital



Präsenz

Wie? Angriffsvektoren

- Einbruch / Diebstahl
- BadUSB
- Shouldersurfing
- Social Engineering



Präsenz

Begriffsklärung

- Blackhat (=„Die Bösen“)
 - Greifen Systeme an für den eigenen Vorteil (Geld, ...)
- Greyhat
 - Greifen Systeme an für einen Sicherheitsgewinn. Ignorieren dabei ggf. Gesetze und Verbote.
- Whitehat (=„Die Guten“)
 - IT-Sicherheitspezialisten, die Systeme absichern wollen. Halten sich an Gesetze und Verbote
- Scriptkiddy
 - Haben nur geringe IT-Kenntnisse, nutzen vorgefertigte Software