Slide 1 - Präsentation über Sicherheitsvorfälle

Worauf muss man achten

Was sind die Möglichkeiten für Hacker

Slide 2 – Wichtige Grundregeln vorweg

Seid aufmerksam bei unbekannten Absendern

Updated eure Programme sowie Virenschutz

Passt auf, wem ihr eure Informationen freigebt

Slide 3 – Unautorisierter Zugriff von Daten und Passwörtern

Hierbei werden Zugriffsberechtigungen missbraucht oder erschlichen

Das Stehlen von schwachen Passwörtern zählt dazu oder wenn man keins benutzt

Brute-Force Angriff also reines per Hand oder maschinelles Ausprobieren von Passwortlisten ausm Netz

Vertrauliche Daten auf die Zugegriffen werden, auf die eigentlich keiner Zugriff haben sollte

unautorisierte Login-Versuche mithilfe von gegebenen oder eher erschlichenen Zugangsdaten

Slide 4 – Unautorisierter Zutritt in verschiedene Accounts

Dazu zählt Einbruch in Accounts

Missbrauch von Zugangskarten

Erschleichung von Schlüsseln

Unautorisierte Weitergabe von Schlüssel oder Zugangskarten an dritte un unbefugte

Verstoß gegen Zutrittsregelungen

Slide 5 - Prävention für solche Zutritte und Zugriffe

Passwörter regelmäßig ändern

Beispielsweise aufm PC nur einen Admin User aktiv nutzen, wenn man es auch wirklich braucht

Unbenötigte Berechtigungen wieder entziehen

Und zuletzt Zugriffe generell reduzieren

Slide 6 – Spam

Dabei meint man das massenhafte Versenden von Mails, Nachrichten, usw. mit der Absicht Leute zu betrügen oder unerwünschte Inhalte zu verbreiten/zeigen

Hierbei wird Spam über lokale IPs oder SMTP-Relays, also ein Mailserver versendet.

Genauso können diese von außen eindringen, E-Mails darf jeder schreiben

Slide 7 – Spam verhindern

Einen Spamfilter aufsetzen, viele Dienste haben bereits einen, welcher aber nicht immer ausreicht

Seine E-Mail nicht überall angeben oder sogar eine temporäre 10 Minuten-mail nutzen für nicht so wichtige Dienste

Dienstliche und private E-Mail separat nutzen

Slide 8 – Phishing

Phishing ist ein betrügerischer Versuch durch bspw. Fake-Webseiten die eine richtige Website imitieren, wobei man seine Daten wie E-Mail & Passwörter eintippt und diese dann weitergeleitet werden an die Betrüger

Slide 9 – Phishing Prävention

E-Mail-Absender prüfen und nicht einfach so auf vorhandene Links clicken, genauso wenig Dateien einfach so herunterladen und erst recht nicht direkt öffnen.

Slide 10 – Social Engineering

Hierbei versuchen Betrüger durch soziale Interaktion dazu, dass ein Opfer freiwillig seine Daten freigibt, dies passiert bspw. indem jemand sich durch öffentliche Information wie auf Linked-In oder Instagram eine fake, aber glaubwürdige E-Mail schreibt, um dadurch Daten zu erhalten.

Slide 11 - Prävention

Gebt nicht zu viel von euch selbst im Internet preis, am besten so wenig Dienstliche Informationen wie nur möglich. Sensible Daten immer im Blick behalten und vieles Hinterfragen.

Slide 12 – Schadsoftware

Viren, welche versuchen ungemerkt Schäden anzurichten

Trojaner, welche zukünftige Angriffe erleichtern indem sie eine Backdoor im System installieren, dadurch kommt man schneller wieder in das gehackte System

Keylogger, speichert jede Eingabe mit der Tastatur, wodurch sich Passwörter leicht erschleichen lassen

Rootkit, verbirgt Anmeldeversuche, Prozesse und Dateien

Adware, zeigt unerwünschte Werbung auf eine nervige Weise

Ransomware, welches alle Dateien im System verschlüsselt und nur für einen Geldbetrag in Krypto wieder entschlüsselt werden kann

Slide 13 - Prävention

Darauf achten was man downloaded, Antivirusprogramm updaten, Browser updaten

BACKUPS ERSTELLEN!

Slide 14 – Scan und Monitoring

Hierbei wird man im wahrsten Sinne des Wortes Überwacht und die Daten werden gesichert

Ports werden gescannt um eine Sicherheitslücken zu finden, genauso beim Vulnerability scanning

und unautorisiertes Monitoring von Daten

Slide 15 – Das wars danke <3