DORNBACH
Unsere Kompetenz – Ihre Zukunft

UNSERE KOMPETENZ - IHRE ZUKUNFT

DORNBACH IT SYSTEMS AG

Cybersicherheit für den Mittelstand

AGENDA

DORNBACH
Unsere Kompetenz – Ihre Zukunft

I. Dornbach IT Systems

II. Welche typischen Angreifer gibt es und welche Motivation haben diese?

III. Das Internet, Gefahr für den Mittelstand?

IV. Angriffsmethoden

V. Was muss getan werden?

VI. Was kann verbessert werden?

VII. Fragen?

DORNBACH IT SYSTEMS AG

DORNBACH
Unsere Kompetenz – Ihre Zukunft

- IT-Dienstleistungsunternehmen der Dr. Dornbach Treuhand GmbH, Bad Homburg
- Betreuung der internen IT der Dornbach Gruppe an (Bad Homburg, Mainz, Darmstadt, Wetzlar, Pforzheim)
- Betreuung von IT-Systemen der Mandanten der Dornbach Gruppe
- IT-Consultingleistungen für Mandanten der Dornbach Gruppe mit Schwerpunkt im Bereich IT-Sicherheit, Digitalisierung, Datenschutz und Datev
- Vorstand Thomas Kern und Patrick Baumann

ANGREIFER AUF IT-SYSTEME

DORNBACH
Unsere Kompetenz – Ihre Zukunft

WER SIND DIE ANGREIFER UND WELCHE MOTIVATION HABEN DIESE?

- **Der Einzeltäter**
  Unterscheidung von „Scriptkiddies“ und professionell agierenden Tätern
  Motivation oft ohne finanziellen Anreiz, „Weil ich es kann!“
- **Kriminelle Organisationen**
  Agieren höchst professionell. Sind meist Dienstleister für andere
  Die Motivation ist der Angriff als Geschäftsmodell (Auftragshacker) oder mit erbeuteten Daten oder Zugängen Geld zu verdienen
- **Kommerzielle Organisationen**
  Möchten sich bereichern oder anderen Schaden zufügen, um selber Vorteile zu haben
  Sind die Auftraggeber der „Auftragshacker“
- **Behörden bzw. Geheimdienste**
  Agieren im Auftrag der jeweiligen staatlichen Regierungen
  In der Regel ist die Legitimation das Gesetz der Staaten
  Es gibt Staaten, die auch Interesse an Wirtschaftsspionage haben

DAS INTERNET

GEFAHR FÜR DEN MITTELSTAND?

DORNBACH
Unsere Kompetenz – Ihre Zukunft

- **Warum ist der Mittelstand Ziel von Angriffen?**
- Der Mittelstand hat meist hochinnovative Entwicklungen und Produkte mit Alleinstellungsmerkmalen.
- **Er ist vergleichsweise schlecht vor Cyberangriffen geschützt! Warum?**
- Gegenüber großen Kapitalgesellschaften vergleichsweise geringes Budget
- Die Mitarbeiter der internen IT-Abteilung sind oft in diesem Bereich nicht gut ausgebildet. Fachpersonal für IT-Sicherheit ist derzeit am Arbeitsmarkt kaum zu bekommen
- Die eigene IT-Abteilung ist „allmächtig“ und wird selten fachlich / technisch kontrolliert
- Externe Hilfe wird nicht angefordert, auch um die eigene Kompetenz nicht in Frage zu stellen
- Auch externe IT-Dienstleister sind selten für IT-Sicherheit spezialisiert
- Externe IT-Dienstleister können teilweise die notwendigen Maßnahmen nicht umsetzen, da sie das Budget nicht bekommen. „Der Externe will nur verkaufen“
- Schlecht geschulte Mitarbeiter sind eine Gefahr!

ANGRIFFSMETHODEN

WELCHE ARTEN VON ANGRIFFEN GIBT ES?

DORNBACH
Unsere Kompetenz – Ihre Zukunft

- Angriffe auf Zugangsdaten mittels Brute Force Attacke
- Ausnutzen von Sicherheitslücken
- Schadprogramme (Malware)
  Viren, Würmer, Trojaner, Spyware, Scareware, Backdoor, Ransomware
- Phishing
  Abgreifen von Benutzerdaten
- Sniffing
  Abgreifen von Datenverkehr
- Spoofing
  Vortäuschung einer anderen Identität
- Man-in-the-Middle
- Denial of Service (DoS)
- Social Engineering
- Abgreifen von Daten über eingeräumte Zugriffsrechte

WAS MUSS GETAN WERDEN?

DIE PFLICHTAUFGABEN DER IT-SICHERHEIT

DORNBACH
Unsere Kompetenz – Ihre Zukunft

- Bestandsaufnahme der IT-Systeme – Wo liegen die Daten?
- Erstellen eines IT-Sicherheitskonzepts. Erarbeiten Sie Maßnahmen!
- Setzen Sie die Maßnahmen auch um!
- Installieren Sie regelmäßig Updates auf allen Ihren IT-Systemen
- Aktuelle Sicherheitssoftware mit Verhaltensanalyse
- Reine Paketfilter Firewallsysteme reichen nicht mehr aus! Die „Fritzbox“ hat als Firewall im Firmenumfeld ausgedient. Die Firewall muss den Datenverkehr analysieren und Vorgänge protokollieren können.
- Nutzen Sie die Protokollierungsfunktionen der Sicherheitssysteme und kontrollieren Sie diese regelmäßig. Nutzen Sie hierfür Anzeigefilter oder Alarmmechanismen.
- Zugriffe von außen auf das Netzwerk nur mit 2-Faktor-Authentifizierung

WAS MUSS GETAN WERDEN?

DIE PFLICHTAUFGABEN DER IT-SICHERHEIT

DORNBACH
Unsere Kompetenz – Ihre Zukunft

- Kontrolle der IT-Sicherheit an kritischen Stellen durch eine 2. Person oder externen Dienstleister (z.B. Firewallregeln, VPN Zugriff) – 4-Augen Prinzip
  Dokumentieren Sie Änderungen
- Minimierung von Zugriffen auf das Netzwerk auch vom gesicherten internen Bereich
- Nur genutzte Datenanschlüsse „patchen“. Insbesondere in halböffentlichen Bereichen
- Trennen Sie Büro-/Verwaltungsnetze von Produktionsnetzen
- Nutzen Sie die Sicherheitsmerkmale der vorhandenen Systeme (z.B. Portsecurity)
- WLAN mit Zugriff auf das Unternehmensnetzwerk niemals mit PSK
- Getrennte WLAN für Gäste ohne Zugriff auf das Unternehmensnetzwerk einrichten

WAS MUSS GETAN WERDEN?

DIE PFLICHTAUFGABEN DER IT-SICHERHEIT

DORNBACH
Unsere Kompetenz – Ihre Zukunft

- Nutzen Sie keine unverschlüsselten mobilen Geräte oder externe Datenträger
- Schützen Sie alle Systeme mit komplexen Kennwörtern (auch UEFI bzw. BIOS Einstellungen)
- Minimierung von Zugriffsrechten der Mitarbeiter auf die IT-Systeme und IT-Software
- Regelmäßige Überprüfung und Aktualisierung des IT-Sicherheitskonzepts
- Mitarbeiter schulen und Leitfaden zu IT-Nutzung erstellen

WAS KANN VERBESSERT WERDEN

DORNBACH
Unsere Kompetenz – Ihre Zukunft

WIE KANN ICH MEIN UNTERNEHMEN NOCH BESSER ABSICHERN ?

- IT-Sicherheitstests:
- Automatisiertes Überprüfen von Zugriffsmöglichkeiten auf die Systeme
- Automatisiertes Überprüfen auf bekannte Schwachstellen der Systeme
- Besser: Zusätzlich regelmäßige manuelle Analyse der IT-Sicherheit
- Achtung: Penetrationstests können auch Schaden anrichten
- Setzen Sie die für Sie zutreffenden Maßnahmen des BSI IT-Grundschutzes um

WAS KANN VERBESSERT WERDEN

DORNBACH
Unsere Kompetenz – Ihre Zukunft

WIE KANN ICH MEIN UNTERNEHMEN NOCH BESSER ABSICHERN ?

- Die interne IT-Abteilung durch externe Berater im Bereich IT-Sicherheit sensibilisieren und ausbilden
- Verträge mit externen IT-Dienstleistern im Bereich IT-Sicherheit präzisieren – Wer ist zuständig?
- Fortlaufende Audits der IT-Sicherheit von externen, spezialisierten Beratern durchführen lassen.
- Prozesse präzisieren und Zugriffsrechte möglichst fein granulieren
- Dazu zählt auch der Zugriff auf die Hardware (z.B. USB Ports)
- Zugriffsrechte der Mitarbeiter über einen Freigabeprozess definieren und automatisiert erfassen und regelmäßig auf die Rechtmäßigkeit und die Notwendigkeit überprüfen (Rezertifizierung).

DORNBACH
Unsere Kompetenz – Ihre Zukunft

UNSERE KOMPETENZ - IHRE ZUKUNFT

FRAGEN?

WWW.DORNBACH-IT-SYSTEMS.DE