10 00 LASST UNS PATCHEN!

< Sicherheitslücken gehören zum IT-Alltag. Aus diesem Grund ist es sehr wichtig, möglichst rasch zu patchen und bekannte Schwachstellen zu reparieren. Erkunden Sie selbst über Suchmaschinen den eigenen Perimeter und bringen Sie Hersteller-Hinweise über Sicherheitslücken rechtzeitig in Erfahrung.

Seien Sie sich bewusst, dass Angreifer oft mehr über Ihre Systeme und die dabei bestehenden Exploits kennen als Ihnen lieb sein dürfte. />

10 01 SIND MOBILE GERÄTE GEFÄHRLICH?

< Mobile Anwendungen und Geräte müssen mit Bedacht eingesetzt werden. Ein Mobile Device Management hilft Ihnen dabei, eine einheitliche Sicherheits-Policy auf alle eingesetzte Geräte zu bringen. Auf "Bring-your-own-device" sollte weitestgehend verzichtet werden, da sich dieses Verfahren kaum sicher um- bzw. einsetzen lässt.

Mit einer sog. Whitelist können Sie kontrollieren, welche Apps auf den Geräten zulässig sind. Gezielte Datenschutzprüfungen bringen Ihnen im Zweifelsfall die nötige Klarheit über mögliche Bedrohungen bei Apps (z.B. Diebstahl von Geschäftskontakten). />

10 10 DATENABFLÜSSE IM AUGE BEHALTEN!

< Wem teilen Sie eigentlich alles Ihre Suchanfragen und Aktivitäten mit? Die Daten, die Ihr Unternehmen verlassen, verraten sehr viel über Ihr Arbeitsgebiet und mögliche Projekte. Versuchen Sie, Ihre Kommunikation nach außen zu begrenzen, indem Sie z.B. Anwendungen sperren und Ports schließen. Verfahren zur Data Loss Prevention können dabei hilfreich sein. Achten Sie dabei auf ein gesundes Gleichgewicht zwischen Datenüberwachung und Mitarbeiterkontrolle. Regeln Sie zudem gezielt den Umgang mit Suchmaschinen und Einträgen in sozialen Netzwerken in Ihrem Unternehmen. />

IMAGE-VERLUST, GEHEIMNIS-OFFENBARUNG, FINANZIELLER SCHADEN ODER GAR DIE INSOLVENZ.

DAS ALLES KANN IHNEN DROHEN, WENN SIE DIE GEFAHR DES CYBERCRIME ZU SPÄT ERKENNEN UND NICHT VORBEREITET SIND.

NUTZEN SIE DIE MÖGLICHKEIT, UM SICH NOCH RECHTZEITIG ZU POSITIONIEREN UND ANGREIFERN DEN DATENDIEBSTAHL IN IHREM UNTERNEHMEN ZU ERSCHWEREN.
WWW.LDA.BAYERN.DE/CYBERCRIME

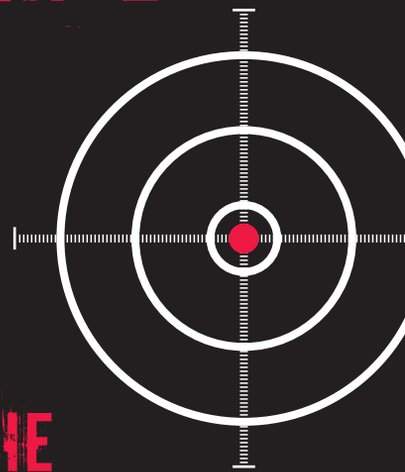
Herausgeber des Flyers:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27, 91522 Ansbach

Tel.: 0981 53 1300
Fax: 0981 53 5300
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT

```
~# HYDRA SSH2 -S 22 -L USERS.TXT -P PASSWORDS.TXT -E
   NS -T 10 ADMIN.MEINEFIRMA.DE
~# MSF > USE EXPLOIT/WINDOWS/SCADA/SCADA_REVERSE
~# NMAP P1433 -SCRIPT MS-SQL-INFO APPBACKEND.MEINEFIRMA.DE
~# SQLMAP.PY -U
   HTTP://WEBSHOP.MEINEFIRMA.DE/PAGE.PHP?ULNPARAM=CONTENT
~# SSLSNIFF -A -C FAKE_CA.PEM -S 444 -W VERTRAULICHE_DATEN.TXT
```

CYBERCRIME BETRIFFT JEDEN



SCHÜTZEN SIE IHR UNTERNEHMEN

00 01 NA SICHER, CHEF!

< IT-Sicherheit ist absolute Chefsache. Ohne konsequente Unterstützung und Vorgabe der Unternehmensleitung kann keine dauerhaft ausreichende Sicherheit für Ihr Unternehmen gewährleistet werden.

Notwendig ist hierbei vor allem das Erstellen, Pflegen und (Vor-)Leben einer umfassenden IT-Sicherheitsleit- und -richtlinie.

Lernen Sie dadurch die eigenen Sicherheitsbedürfnisse und -anforderungen kennen und sensibilisieren Sie Ihre Mitarbeiter.

Sicherheit ohne Chef gibt es nicht! />

00 10 WIR BRAUCHEN EINEN PROZESS!

< Um Sicherheit strukturiert und effizient zu organisieren, ist es notwendig, einen geregelten Prozess zur IT-Sicherheit als festen Bestandteil in Ihren Unternehmensalltag einfließen zu lassen. Ein IT-Sicherheitsbeauftragter, ausgestattet mit den erforderlichen Ressourcen, sorgt für dessen Umsetzung. />

00 11 OHNE TOOLS GEHT GAR NICHTS!

< Essentiell ist auch der Einsatz effektiver Sicherheitswerkzeuge, die es Ihnen ermöglichen, gegen unterschiedliche Angriffstypen stand zu halten und Ihre Daten zu schützen.

Eine geeignete Firewallarchitektur (Richtig konfiguriert!), der Einsatz von Virenscannern (Erkennen nicht alles!) und ggf. Intrusion Detection Systeme (Verwaltungsaufwand nicht unterschätzen!) bilden hierbei die Grundausstattung. />

01 00 WER GREIFT UNS AN?

< Wissen Sie eigentlich, mit wem Sie es zu tun haben? Potentielle Angreifer kommen aus allen Schichten:

~ Mitarbeiter aus unterschiedlichen Motiven
#Frust, Neugierde, Rache

~ Technisch Nicht-versierte mit 1-Klick-Angriffstool
#Skript-Kiddie

~ Technisch motivierte Personen mit hohem Know-How
#Hacker

~ Gruppen zur Durchsetzung politischer Interessen
#Hacktivism

~ Organisierte Banden mit umfangreicher Ausstattung
#Cyber-Kriminielle

~ Staatliche Stellen mit unbegrenzten Ressourcen
#Nachrichtendienste

~ Wettbewerber
#Neider />

01 01 WO UND WIE ATTACKIERT MAN UNS?

< Cyber-Angriffe können von allen Seiten stattfinden:

Auf Netzwerkebene:
>> z.B. Firewall, Webserver, Datenbank

Bei Anwendungen:
>> z.B. SQL-Injection, XSS, CSRF

Über Kommunikationskanäle:
>> z.B. Phishing, Man-In-The-Middle, Advanced Persistent Threads

Durch Schadsoftware:
>> z.B. Drive-By-Download, per PDF, Mail-Anhang, USB-Stick

Bei der Entsorgung:
>> z.B. Rekonstruktion von gelöschten Festplatten, Rückgabe von Leasing-Geräten, Unzureichende Aktenvernichtung

Mittels Social Engineering:
>> z.B. telefonisch, in sozialen Netzwerken />

01 10 WIR MÜSSEN VERSCHLÜSSELN!

< Krypthographie funktioniert! Denken Sie daran,
- Unternehmensnetze sicher zu verbinden (VPN)
- Datenträger zu verschlüsseln (z.B. AES-256 Bit)
- Webanwendungen abzusichern (HTTPS, HSTS, Secure-Cookie-Flag)
- STARTTLS beim Mailserver zu konfigurieren
- Ende-Zu-Ende Verschlüsselung einzusetzen (z.B. S/MIME mit 2048 Bit)
- Drahtlose Netze richtig zu betreiben (WPA2 mit 20-stelligem Passwort)
- Daten vor der Ablage in der Cloud zu verschlüsseln (z.B. AES-256 Bit)
- Passworte sicher zu speichern (z.B. PBKDF2)
- Entschlüsselungsversuche mit Perfect Forward Secrecy zu erschweren />

01 11 WER IST FÜR WAS BERECHTIGT?

< A und O eines durchgängigen Sicherheitskonzepts ist ein sauber gepflegtes Berechtigungsmanagement ohne "Leichen". Hierbei sollte nach dem Motto verfahren werden: Nur die absolut erforderlichen Rechte erteilen.

Gruppenkennungen sind zu vermeiden, da damit eine belastbare Vorgangsprotokollierung nicht möglich ist.

Insbesondere bei administrativen Kennungen muss eine sehr strenge Reglementierung und Vergabepraxis erfolgen. Bei Daten mit erhöhtem Schutzbedarf sollte zudem das Vier-Augen-Prinzip berücksichtigt werden, um internen Datendiebstahl durch einzelne Personen zu erschweren. />