UpGreat
we know-how to do IT

# AUDYTY BEZPIECZEŃSTWA

## ZADBAJ O BEZPIECZEŃSTWO WSZYSTKICH PROCESÓW W TWOJEJ FIRMIE

Bezpieczeństwo systemów teleinformatycznych jest obszarem, któremu najczęściej poświęca się zbyt mało czasu i uwagi. Według raportu PwC 96% firm doświadczyło ponad 50 incydentów naruszenia bezpieczeństwa w ostatnich latach. Kwestie bezpieczeństwa są często bagatelizowane ze względu na brak środków finansowych, wolnych etatów i złudne poczucie, że posiadanie firewalla i programów antywirusowych załatwia kwestię bezpieczeństwa w dostatecznym stopniu, a tymczasem aż 79% incydentów w firmach powodują aktualni pracownicy.

Obecnie od bezpieczeństwa środowiska IT (jak i również OT - procesy produkcyjne są coraz bardziej zagrożone) zależne jest dzisiaj bezpieczeństwo wszystkich procesów biznesowych, danych i komunikacji czyli w efekcie bezpieczeństwo całej firmy i jej pracowników. Odpowiedzialność prawna np. za wyciek danych osobowych lub utrata dobrego wizerunku firmy związana z nagłaśnianymi chętnie przez media incydentami bezpieczeństwa to tylko niektóre z przykrych konsekwencji zaniedbań.

Bezpieczeństwo IT

Architektura IT

Outsourcing IT

# AUDYTY BEZPIECZEŃSTWA

## ZADBAJ O BEZPIECZEŃSTWO WSZYSTKICH PROCESÓW W TWOJEJ FIRMIE

### Testy penetracyjne

W sposób praktyczny badamy poziom bezpieczeństwa środowiska IT i obnażamy jego słabe elementy. W ramach testów badane są m.in. takie elementy infrastruktury jak sieci kablowe i bezprzewodowe, serwery, urządzenia sieciowe, stacje robocze.

### Zgodność z międzynarodowymi normami ISO

Kwestie bezpieczeństwa regulowane są przez niektóre z norm ISO, takie jak np. ISO 27001 (System Zarządzania Bezpieczeństwem Informacji) czy ISO 27002 (dawniej ISO 17799 - Praktyczne zasady zarządzania bezpieczeństwem informacji).

### Inwentaryzacja oprogramowania

Brak kontroli nad instalowanym i używanym w firmie oprogramowaniem poza konsekwencjami prawnymi wynikającymi z naruszeń licencyjnych pociąga za sobą również ryzyko aktywowania narzędzi o charakterze koni trojańskich mających na celu szpiegowanie i wykradanie informacji.

### Badanie bezpieczeństwa systemów webowych

Audyt mający na celu ustalenie czy mechanizmy uwierzytelniania i wprowadzania danych w aplikacjach webowych gwarantują bezpieczeństwo i odporność na określonego typu ataki.

**Polityka bezpieczeństwa** to opracowanie zawierające zbiór zasad mających na celu ochronę systemu informacyjnego firmy.

### Badanie odporności użytkowników na socjotechniki

Audyt mający na celu ustalenie w jakim stopniu pracownicy firmy podatni są na ataki socjotechniczne. W trakcie audytu stosowane są kontrolowane próby pozyskania od użytkowników poufnych informacji.

### Zgodność z krajowymi przepisami prawa

Obecnie firmy z sektora prywatnego oraz jednostki publiczne mają obowiązek związany ze zgłaszaniem do GIODO baz danych osobowych, wdrażaniem polityk bezpieczeństwa czy corocznym wykonywaniem audytów bezpieczeństwa.

### Testy bezpieczeństwa sieci bezprzewodowej

Audyt obejmuje zagadnienia związane z bezpieczeństwem sieci WLAN. Pod uwagę brana jest np. możliwość podsłuchania lub zakłócenia ruchu w sieci bezprzewodowej z poza terenu firmy, z wykorzystaniem anten i urządzeń o większej mocy sygnału niż tradycyjne karty sieciowe.

### Skanowanie systemów pod kątem luk bezpieczeństwa

Audyt mający na celu ustalenie na jakiego typu zagrożenia podatne są systemy operacyjne stosowane na serwerach i stacjach roboczych.

**Opieka Security Officera** w formie cyklicznej usługi zapewnia odpowiednią ochronę zasobów informacyjnych i technologicznych oraz procesów biznesowych.

UpGreat
we know-how to do IT

61 664 16 20
biuro@upgreat.pl
upgreat.poznan
www.upgreat.pl