

Cyber Security

Umfassende IT-Sicherheitsberatung für Ihr Unternehmen



```
money_satang / 0.50);  
- 0.50);
```

```
money_satang / 0.25);  
- 0.25);
```

```
change) * (money_satang * 100);
```

```
float r;  
float area;
```

```
printf("input value of radius : ");  
scanf("%f", &r);
```

```
area = (M_PI * (r * r)) / 2;
```

```
printf("\n Area of the semicircle = %2f\n\n", area);
```

```
return 0;
```

```
int hexagonSize;  
int i, s;  
  
printf(" Enter number for hexagon size: ");  
scanf("%d", &hexagonSize);  
  
for(i=0; i<hexagonSize; i++)  
{  
    for(s=0; s<hexagonSize-i; s++)  
        printf(" ");  
}
```

```
int hexagonSize;  
int r, s, i;
```

```
printf(" Enter number for Hexagon size: ");  
scanf("%d", &hexagonSize);
```

```
for(r=0; r<hexagonSize; r++)  
{  
    for(s=0; s<hexagonSize-r; s++)  
        printf(" ");  
}
```

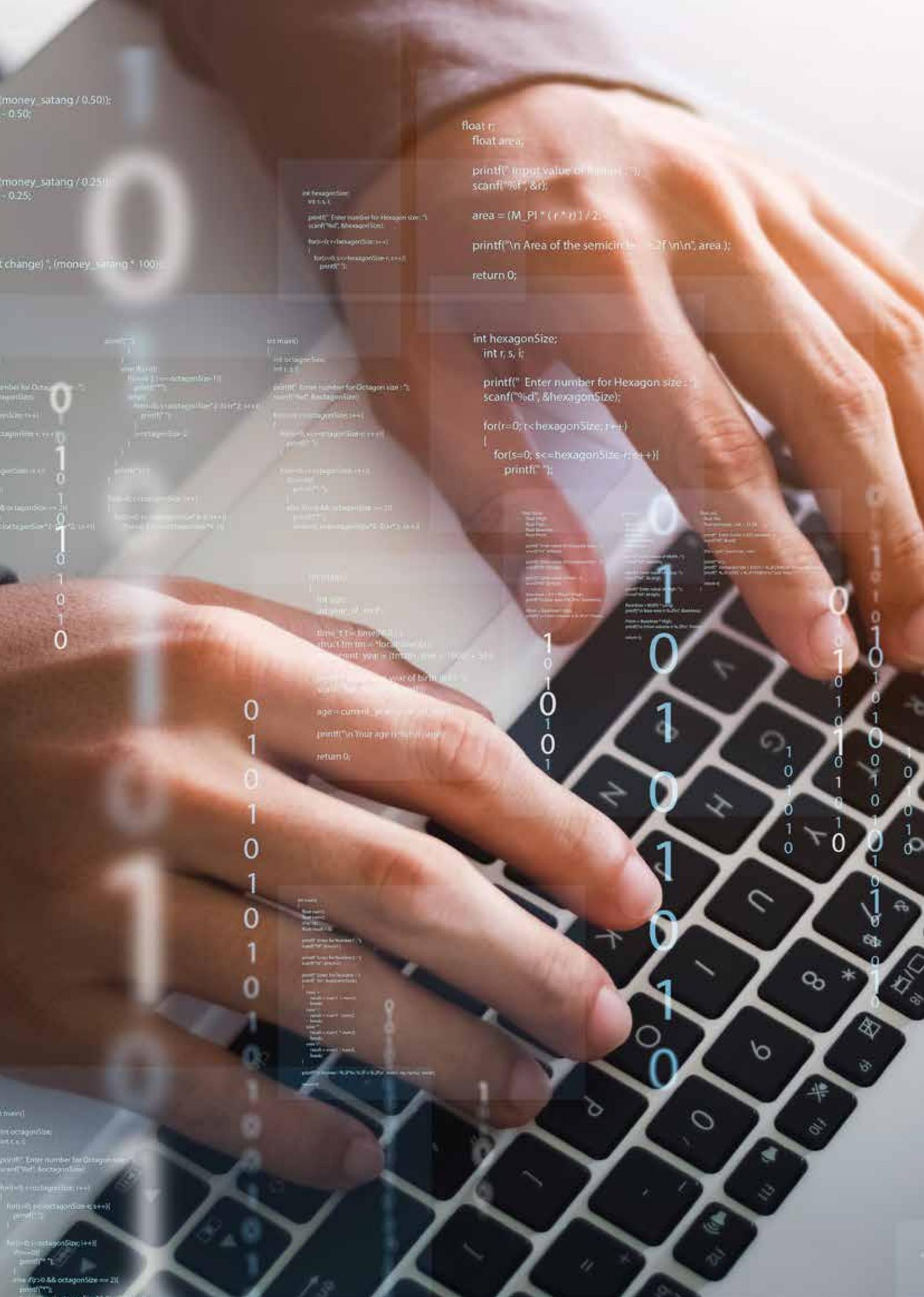
```
int main()  
{  
    int octagonSize;  
    int i, s;  
  
    printf(" Enter number for Octagon size: ");  
    scanf("%d", &octagonSize);  
  
    for(i=0; i<octagonSize; i++)  
    {  
        for(s=0; s<octagonSize-i; s++)  
            printf(" ");  
    }
```

```
int main()  
{  
    int age;  
    int year_of_birth;  
  
    printf("Enter your age: ");  
    scanf("%d", &age);  
  
    printf("Enter your year of birth: ");  
    scanf("%d", &year_of_birth);  
  
    int current_year = 2024;  
    int current_age = current_year - year_of_birth;  
  
    printf("Your age is %d years.", age);  
  
    return 0;  
}
```

```
int main()  
{  
    int octagonSize;  
    int i, s;  
  
    printf(" Enter number for Octagon size: ");  
    scanf("%d", &octagonSize);  
  
    for(i=0; i<octagonSize; i++)  
    {  
        for(s=0; s<octagonSize-i; s++)  
            printf(" ");  
    }
```

```
int main()  
{  
    int octagonSize;  
    int i, s;  
  
    printf(" Enter number for Octagon size: ");  
    scanf("%d", &octagonSize);  
  
    for(i=0; i<octagonSize; i++)  
    {  
        for(s=0; s<octagonSize-i; s++)  
            printf(" ");  
    }
```

```
int main()  
{  
    int octagonSize;  
    int i, s;  
  
    printf(" Enter number for Octagon size: ");  
    scanf("%d", &octagonSize);  
  
    for(i=0; i<octagonSize; i++)  
    {  
        for(s=0; s<octagonSize-i; s++)  
            printf(" ");  
    }
```



Umfassende IT-Sicherheit für Ihr Unternehmen.

Trotz des Wissens um Cyber- und IT-Risiken besitzen viele Unternehmen noch keine umfassende Strategie zur Informations- und IT-Sicherheit.

Warum ist Cyber Security so wichtig?

Die stetig wachsende Menge an Daten und Informationen zählt heute oft zu den wichtigsten Unternehmenswerten, die vor Diebstahl und Manipulation geschützt werden müssen. Wer die Sicherheit seiner IT-Systeme und Daten gewährleisten will, sollte sich daher mehrere Fragen stellen:

- Ist das Sicherheitsniveau unserer IT-Landschaft angemessen?
- Haben wir alle wesentlichen Cyber-Risiken adressiert?
- Sind unsere Daten ausreichend gegen Cyberangriffe und Diebstahl durch unbefugte Dritte und Innentäter:innen abgesichert?
- Haben unsere Prozesse und Systeme Schwachstellen?
- Entsprechen unsere Maßnahmen für Cyber/IT-Sicherheit den tatsächlichen Bedrohungen?
- Sind unsere Mitarbeiter:innen ausreichend auf die Gefahren vorbereitet?
- Können das Unternehmen und die Mitarbeiter:innen unmittelbar und richtig auf Angriffe reagieren?

Unsere Lösung für Ihre Sicherheit

Wir helfen Ihnen, Ihr Unternehmen umfassend gegen die Gefahren im Bereich der Cyber/IT-Sicherheit zu wappnen.

Präventiv

im Rahmen einer IT-/Cyber-Sicherheitsanalyse.

- Awareness-Schulungen
- Cyber Risk Assessment
- Malware-Analyse
- ISMS
- IT Security

Proaktiv

in der Entwicklung einer auf Sicherheit orientierten IT-Strategie und einem Vulnerability Assessment.

- Penetration Testing
- Vulnerability Assessment
- Business Continuity

Reaktiv

unterstützen Sie unsere erfahrenen Expertinnen aus den Bereichen Digital Advisory und Forensic dabei, rasch auf Cyber-Attacks zu reagieren. Unter dem Begriff "Cyber Incident Response" wird das Auffinden und Schließen von Sicherheitslücken, die Aufklärung von Attacks, die Ermittlung der entstandenen Schäden sowie die Zurückverfolgung des Angriffs zusammengefasst.

Im Ernstfall beraten Sie unsere Expertinnen nicht nur bei der Wiederherstellung Ihrer Systeme, sondern auch zu Haftungsfragen, mit Beweissicherungen, der Abwicklung mit Versicherern und in datenschutzrechtlichen Belangen.



Unsere 24h-Rückruf-Hotline

01 / 505 43 13 4444



Cyber Security Services.

Um Ihr Unternehmen optimal vor Cyber/IT-Risiken und -Gefahren zu schützen, bieten wir Ihnen eine Reihe von Beratungsleistungen.

Cyber / IT Security Audit

Unser ganzheitliches Cyber / IT Security Audit hilft Ihnen, einen besseren Überblick über mögliche Schwachstellen Ihrer IT-Organisation, -Prozesse und -Systeme zu gewinnen. Gemeinsam mit Ihrer IT-Abteilung erstellen wir eine Bestandsaufnahme von Organisation, Prozessen, Systemen und bereits vorhandenen technischen und operativen Sicherheitsmechanismen. Dabei evaluieren wir auch alle sicherheitsrelevanten Prozesse, wie beispielsweise das Patch-Management, die Datensicherung oder das Mobile-Device-Management und helfen bei der richtigen Konfiguration von Systemen und Sicherheitsmechanismen, wie beispielsweise Firewalls. Auf Wunsch beraten wir Sie auch in der Planung Ihres Netzwerks unter Sicherheitsaspekten, zum Beispiel, um besonders sensible Systeme wie Produktionssteuerungen (Industrie 4.0, IOT) in eigenen Subnetzen zu segregieren.

Schwachstellenanalyse

Bei einer Schwachstellenanalyse überprüfen wir Ihre IT-Systeme mit Hilfe marktführender Tools auf bekannte Schwachstellen, Fehlkonfigurationen und operative Sicherheitsrisiken, wie beispielsweise schwache Passwörter oder veraltete Software. Dabei prüfen wir sowohl aus der Perspektive eines externen Angriffs als auch aus der Innenansicht, um die Perspektive von Mitarbeiter:innen oder Gästen abzubilden. Auch ihre WLAN-Netzwerke unterziehen wir einer ausführlichen Prüfung und decken so zum Beispiel eventuelle Schwachstellen bei der Zugangskontrolle auf.

Penetrationstest / Web-Penetrationstest

Um Ihre IT-Systeme optimal abzusichern, empfehlen wir einen Penetrationstest. Dabei nehmen unsere Expert:innen die Rolle von Angreifer:innen ein und testen, welche Schwachstellen die IT-Systeme in Ihrem Unternehmen aufweisen und auf welche kritischen Systeme und Daten sich dadurch zugreifen lässt.

So decken wir auch Schwachstellen auf, die ein automatischer Scan allein nicht finden würde und sichern Ihr Unternehmen gegenüber gezielten Attacken bestmöglich ab.

Awareness-Schulungen

Eines der größten IT-Sicherheitsrisiken für Unternehmen ist der sorglose Umgang von Mitarbeiter:innen mit Angriffsversuchen per E-Mail oder Social Engineering. So lassen sich zum Beispiel viele Infizierungen mit Erpressungstrojanern (Ransomware) oder Angriffe durch sog. „Fake President Fraud“ verhindern, wenn Mitarbeiter:innen E-Mails mit infizierten Anhängen besser erkennen. Bei unseren Awareness Trainings schulen wir Ihre Mitarbeiter:innen, Angriffsversuche zu erkennen und richtig damit umzugehen. So werden viele Angriffe bereits im ersten Stadium gestoppt.

Ihr Mehrwert

Eine IT-Sicherheitsanalyse durch unsere Expert:innen macht Ihre IT-Systeme widerstandsfähiger gegen die vielfältigen Cyber-Bedrohungen, denen Unternehmen jeden Tag gegenüberstehen. Damit helfen wir Ihnen, eine höhere Ausfallsicherheit der IT-gestützten Prozesse in Ihrem Unternehmen zu erreichen und kritische Daten besser zu schützen. Hacker, Wirtschaftsspione und Innentäter:innen haben es erheblich schwerer, Ihrem Unternehmen zu schaden.

Ihr Ansprechpartner

Unsere Expert:innen bieten maßgeschneiderte Cyber-Security-Lösungen für sichere digitale Assets, nutzen moderne Business Intelligence & Data-Analytics-Tools für wertvolle Erkenntnisse und setzen auf individuelle Softwareentwicklung.



Mag. Georg H. Jeitler, BA MBA CMC
Partner | Head of Forensic Services

T +43 1 505 - 2068

M +43 664 1616388

E georg.jeitler@at.gt.com

Mag. Georg H. Jeitler ist Partner bei Grant Thornton Austria in den Bereichen Advisory und Forensic Services. Er ist seit mehr als 20 Jahren in der Beratung von Unternehmen tätig und hat nationale und internationale Projekte in verschiedensten Branchen sowie im öffentlichen Bereich umgesetzt. Schwerpunkte seiner Beratungstätigkeit sind u.a. allgemeine Strategiefragen, die Optimierung von Compliance-Systemen sowie Anti-Fraud und Antikorruption.

Georg H. Jeitler leitet den Bereich der Forensic Services, was neben allgemeiner Risiko-Beratung sowohl forensische Ermittlungen als auch ein breites Leistungsspektrum in der Digitalforensik umfasst.

Schwerpunkte

- Allgemeine Strategiefragen
- Optimierung von Compliance-Systemen
- Anti-Fraud und Antikorruption
- Forensische Ermittlungen, Internal Investigations
- Implementierung und Betrieb von Hinweisgebersystemen für Whistleblower

