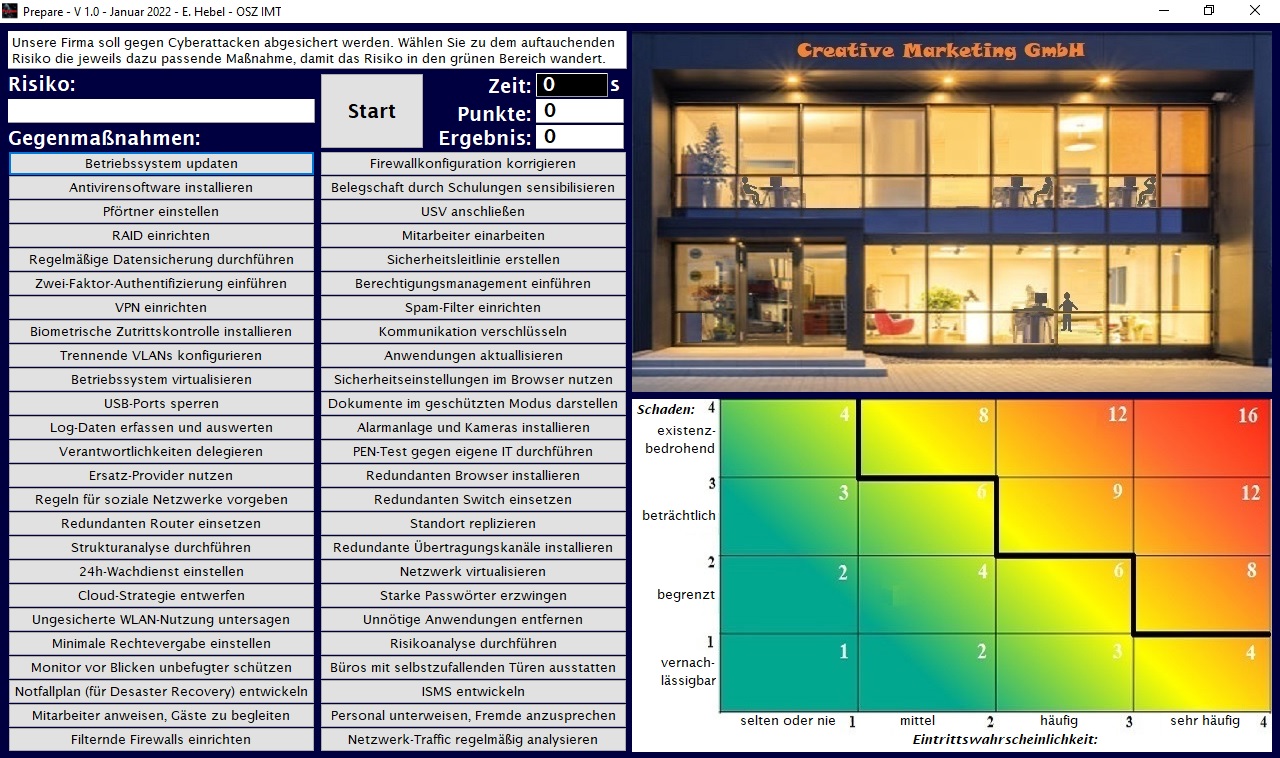
**Lernsituation:** Mit dem Programm „Prepare“ erfahren sie nicht nur, was alles passieren kann in einem Unter-nehmen, wenn die Cybersicherheit vernachlässigt wird, sondern auch, was möglich ist, um sich zu schützen.



**a.)** Beantworten Sie zunächst folgende vorbereitende Fragen (in Partnerarbeit).

**1.)** Was bedeutet Redundanz?

Redundanz bezieht sich auf die Wiederholung von Informationen oder Ressourcen, die für den Fall der Ausfall von Teilen des Systems notwendig sind, um die Funktionsfähigkeit aufrechtzuerhalten oder die Fehlerwahrscheinlichkeit zu reduzieren. In der Informatik wird es oft in Bezug auf Datensicherheit und Netzwerke verwendet.

**2.)** Was ist DDoS?

DDoS steht für "Distributed Denial of Service" und bezieht sich auf eine Art von Cyberangriff, bei dem eine Vielzahl von Computern, die sogenannten "zombie-computer" von einem Angreifer kontrolliert werden, um einen einzelnen Zielcomputer oder ein Netzwerk mit unerwünschtem Traffic zu überfluten. Das Ziel dieses Angriffs ist es, die Verfügbarkeit des Zielcomputers oder Netzwerks zu beeinträchtigen, indem es die Ressourcen des Systems überlastet und dadurch die normale Nutzung unmöglich macht.

**3.)** Was ist ein VPN?

VPN steht für Virtual Private Network, es ist ein privates Netzwerk, das über ein öffentliches Netzwerk, in der Regel das Internet, aufgebaut wird. Ein VPN ermöglicht es Benutzern, sicher auf entfernte Netzwerke und Ressourcen zuzugreifen, indem es eine verschlüsselte Verbindung bereitstellt. Es nutzt dazu Tunneling Protokolle um die Daten zu verschlüsseln und zu authentifizieren. VPNs werden häufig von Unternehmen genutzt, um ihre Mitarbeiter auf Firmennetzwerke und Ressourcen von entfernten Standorten aus zugreifen zu lassen, aber auch von Privatpersonen, um die eigene Anonymität im Internet zu schützen oder geografische Sperren von bestimmten Inhalten zu umgehen.

**4.)** Was ist ein VLAN?

VLAN steht für Virtual Local Area Network. Ein VLAN ist eine logische Gruppe von Geräten in einem physischen Netzwerk, die sich so verhalten, als ob sie in einem eigenen physischen Netzwerk sind, obwohl sie tatsächlich Teil desselben physischen Netzwerks sind. Dies ermöglicht es, dass Nutzer in verschiedenen VLANs nicht direkt miteinander kommunizieren können, es sei denn, es gibt spezielle Konfigurationen, die dies ermöglichen. VLANs werden häufig in Unternehmensnetzwerken verwendet, um die Netzwerksicherheit und die Netzwerkverwaltung zu verbessern, indem sie

die Kommunikation zwischen verschiedenen Teilen des Netzwerks einschränken und die Überwachung von Netzwerkverkehr vereinfachen. Sie können auch verwendet werden, um die Netzwerklast zu reduzieren und die Performance zu verbessern.

**5.)** Was ist ein RAID?

RAID steht für Redundant Array of Independent Disks. Es handelt sich dabei um eine Methode zur Erhöhung der Datensicherheit und/oder Leistung von Datenspeichern durch die Verwendung mehrerer physischer Festplatten in einem einzigen Logischen Volume. RAID-Systeme nutzen verschiedene Techniken wie Mirroring (RAID 1), Striping (RAID 0) oder Parity (RAID 5, RAID 6) um Daten auf mehrere Festplatten zu verteilen und dadurch Datenverlust bei Ausfall einer Festplatte zu minimieren oder Leistung zu erhöhen. Es gibt verschiedene RAID-Levels, die sich durch die Art der Datenredundanz und die Anzahl der benötigten Festplatten unterscheiden.

**6.)** Was ist Biometrie?

Die Technologie der Biometrie wird in vielen Anwendungen eingesetzt, wie z.B. in der Sicherheitsbranche, zur Zutrittskontrolle, in der Verwaltung von Identitäten und Zugriffsberechtigungen und in der Finanzbranche. Biometrische Systeme ermöglichen eine schnelle und sichere Identifizierung von Personen, da sie Merkmale verwenden, die einzigartig und schwer zu fälschen sind. Allerdings gibt es auch Bedenken bezüglich der Privatsphäre und des Schutzes der persönlichen Daten, die durch die Verwendung von Biometrie entstehen können.

**7.)** Was ist eine Standortreplikation?

Standortreplikation bezieht sich auf die Technik zur Synchronisierung von Daten zwischen mehreren Standorten, um eine höhere Verfügbarkeit und Zuverlässigkeit von Daten sicherzustellen. Es ermöglicht es, dass Daten in Echtzeit oder in regelmäßigen Abständen zwischen den Standorten repliziert werden und dadurch ein Backup oder eine Disaster Recovery Lösung bereitgestellt wird. Standortreplikation kann in verschiedenen Konfigurationen eingesetzt werden, wie z.B. der Einsatz von synchroner oder asynchroner Replikation, der Verwendung von unidirektionaler oder bidirektionaler Replikation. Standortreplikation wird häufig von Unternehmen genutzt, die Daten an mehreren Standorten benötigen, um die Verfügbarkeit von Anwendungen und Diensten sicherzustellen, oder die ihre Daten vor Naturkatastrophen, Stromausfällen oder anderen Unterbrechungen schützen möchten.

**8.)** Was ist eine USV?

USV steht für Unterbrechungsfreie Stromversorgung (engl. Uninterruptible Power Supply). Es handelt sich hierbei um eine Art von Stromversorgungsgerät, das eine kontinuierliche Stromversorgung bereitstellt, indem es den Wechsel von der Hauptstromversorgung zu einer internen Batterie oder einem Notstromgenerator automatisch und innerhalb von Millisekunden ermöglicht, wenn es zu einem Ausfall der Hauptstromversorgung kommt. USVs werden häufig in kritischen Anwendungen eingesetzt, wie z.B. in Rechenzentren, Krankenhäusern, Banken und anderen Einrichtungen, die eine kontinuierliche Stromversorgung benötigen, um Ausfälle und Datenverluste zu vermeiden. Sie sind auch in privaten Haushalten nützlich um Geräte wie Router, Modems und Smart-Geräte zu schützen, wenn es zu einem Stromausfall kommt.

**9.)** Was ist ein PEN-Test?

PEN-Test steht für Penetration Testing oder auch Penetrationstest. Es handelt sich hierbei um eine Methode zur Simulation eines Angriffs auf ein Computersystem, ein Netzwerk oder eine Anwendung, um Schwachstellen und Sicherheitslücken zu identifizieren. PEN-Tests werden von Sicherheitsexperten durchgeführt, die versuchen, in das System einzudringen und es auf die gleiche Weise zu nutzen, wie ein Angreifer es tun würde. Das Ziel eines PEN-Tests ist es, die Sicherheit des Systems auf die Probe zu stellen und zu ermitteln, wie gut es gegen unerlaubten Zugriff und Angriffe geschützt ist. PEN-Tests umfassen in der Regel sowohl automatisierte als auch manuelle Tests, um mögliche Schwachstellen in einem System zu identifizieren und zu bewerten. PEN-Tests können auch verwendet werden, um die Wirksamkeit bestehender Sicherheitsmaßnahmen zu überprüfen und um Empfehlungen für die Verbesserung der Sicherheit zu geben.

**10.)** Was bedeutet minimale (restriktive) Rechtevergabe?

Minimale restriktive Rechtevergabe bedeutet, dass ein Benutzer nur die minimal erforderlichen Rechte erhält, um seine Aufgaben auszuführen. Das bedeutet, dass jeder Benutzer nur Zugriff auf die Ressourcen hat, die er zur Erfüllung seiner Aufgaben benötigt und keine zusätzlichen Rechte. Dies ist ein wichtiger Bestandteil von sicherheitskritischen Systemen, da es dazu beiträgt, die Auswirkungen von potenziellen Angriffen oder Fehlern auf ein Minimum zu beschränken. Es ist ein grundlegender Ansatz der Informationssicherheit, der darauf abzielt, das Risiko von Sicherheitsverletzungen zu minimieren, indem das Potenzial für unbefugten Zugriff oder Missbrauch von Ressourcen reduziert wird. Dies kann durch die Verwendung von Rollen- und Berechtigungsmodellen, die die Vergabe von Rechten auf eine bestimmte Gruppe von Benutzern beschränken, erreicht werden.

**b.)** Starten Sie nun das Programm „Prepare.EXE“, um die folgenden Aufgaben bearbeiten zu können.

1.) Ergänzen Sie die Tabelle mit den Informationen aus der Risikomatrix in „Prepare“. Dazu müssen Sie auf die Risiken warten, da diese zufällig erscheinen.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risiko | Eintrittswahr-scheinlichkeit ohne Maßnahme | Schaden | Maßnahme | Eintrittswahr-scheinlichkeit  mit  Maßnahme | Risiko-wert-  änderung | Risiko-  redu-zierung  um |
| Virus wegen  fehlendem  Update | mittel | existenz-bedrohend | Betriebsystem  updaten | selten oder nie | 8 🡪 4 | 50 % |
| PC ohne Strom wegen  Spannungs-ausfall |  |  |  |  |  |  |
| Kundendaten verloren wegen SSD-Crash |  |  |  |  |  |  |
| Werbemails  überfluten E-Mail-Postfächer |  |  |  |  |  |  |
| Virus über Brute-Force-Anttacke |  |  |  |  |  |  |
| Unbefugter im Büro |  |  |  |  |  |  |

**c.)** Bearbeiten Sie nun die abschließenden Aufträge.

**1.)** Schauen Sie auf die Risikomatrix, nachdem Sie „Start“ geklickt haben. Welches sind die höchsten Risiken der Firma?

**2.)** Warum sind die existenzbedrohenden Viren nicht die höchsten Risiken?

**3.)** Wie hoch ist das Risiko, das die Firma noch akzeptiert?

**4.)** Was haben die Maßnahmen 6,7,8,27,28,30,31,32 und 34 gemeinsam?